Universitat de les Illes Balears

Invertim en el seu futur
Unió Europea
Fons Social Europeu

Govern de les Illes Balears
Conselleria d'Innovació, Recerca i Turisme
Direcció General d'Innovació i Recerca

TESIS DOCTORAL
2017

ASPECTOS JURÍDICO-MERCANTILES DE LA SUSCRIPCIÓN DE SERVICIOS DE COMPUTACIÓN EN LA NUBE POR PEQUEÑOS EMPRESARIOS; EN PARTICULAR, IMPLICACIONES EN EL SECTOR TURÍSTICO

Volumen I de II

Francisca María Rosselló Rubert

Universitat de les Illes Balears

Invertim en el seu futur

Unió Europea
Fons Social Europeu

Govern de les Illes Balears
Conselleria d'Innovació, Recerca i Turisme
Direcció General d'Innovació i Recerca

TESIS DOCTORAL
2017

Programa de Doctorado en Derecho

ASPECTOS JURÍDICO-MERCANTILES DE LA SUSCRIPCIÓN DE SERVICIOS DE COMPUTACIÓN EN LA NUBE POR PEQUEÑOS EMPRESARIOS; EN PARTICULAR, IMPLICACIONES EN EL SECTOR TURÍSTICO

Volumen I de II

Francisca María Rosselló Rubert

Directora: Apol·lònia Martínez Nadal
Tutora: Apol·lònia Martínez Nadal

Doctora por la Universitat de les Illes Balears

A mis padres, por haberse esforzado tanto para que tenga una vida feliz y próspera. Son vuestros cualesquiera éxitos que pueda obtener como profesional y como persona.

A mi marido, por demostrarme cada día que nuestro vínculo va más allá de lo explicable, y por su paciencia infinita.

A Catalina, por ser mi mejor guía y consejera.

A mi Pimpi, a mis preciosas "unicornios" Cris, Virgi, Mai, Mayte y Estefi, y a mis hermanas de alma Sahra, Donna, Mary y Nisrine. Vuestros abrazos han impulsado gran parte de este trabajo.

A todas las demás personas y seres que me han acompañado en cuerpo y/o espíritu.

Y, muy especialmente, a mis dos Apolónias. *Per ardua, ad astra.*

RESUM

Aquesta tesi doctoral es centra en la contractació de serveis de computació al núvol en la modalitat d'implementació pública per part del petit empresari, que té lloc en línea i a través de condicions generals. La modalitat de núvol públic permet al petit empresari una implementació económica i senzilla de recursos de computació que es reben mitjançant Internet, on el proveïdor s'encarrega de l'adquisició, manteniment i actualització dels sistemes informàtics que sustenten el servei. El nostre treball pretén donar un tractament uniforme als continguts més habituals dels contractes *cloud* no negociats, i especialment, a les obligacions que integren la relació jurídica entre petit empresari suscriptor i proveïdor dels serveis. D'altra banda, es vol determinar la naturalesa jurídica que es correspongui amb la generalitat dels contractes de núvol públic. Per finalitzar, es proposen solucions a la problemàtica específica derivada d'aquests nous i habituals contractes, relacionades amb la titularitat de les dades migrades, la protecció de la privacitat i el destí de les dades remanents als sistemes del proveïdor quan el contracte s'hagi extingit.

Pel que fa als contractes *cloud* que suscriu el petit empresari del sector turístic, volem recollir els serveis d'implementació de núvol públic més populars, i identificar-ne els aspectes que resulten especialment problemàtics, com la continuitat del servei i els factors de disponibilitat o les repercusions a la reputació de l'establiment o servei turístic.

RESUMEN

Esta tesis doctoral se centra en la contratación de servicios de computación en la nube en su modalidad de implementación pública por parte del pequeño empresario, que tiene lugar en línea y a través de condiciones generales. La modalidad de nube pública permite al pequeño empresario una implementación económica y sencilla de recursos de computación, que recibirá a través de Internet, y en la cual el proveedor se encargará de adquirir, mantener y actualizar los sistemas informáticos que sustentan el servicio. Nuestro trabajo pretende dar un tratamiento

uniforme a los contenidos más habituales de los contratos de computación en la nube no negociados, y, especialmente, a las obligaciones que integran la relación jurídica entre el pequeño empresario suscriptor y el proveedor de servicios. Por otra parte, se quiere determinar la naturaleza jurídica que corresponda a la generalidad de contratos de nube pública. Para acabar, se proponen soluciones a la problemática específica derivada de estos nuevos y extendidos contratos, relacionadas con la titularidad de los datos migrados, la protección de la privacidad y el destino de los datos remanentes en los sistemas del proveedor una vez que el contrato haya llegado a su fin.

Respecto de los contratos *cloud* suscritos por el pequeño empresario del sector turístico, queremos identificar los servicios de implementación de nube pública más populares, y analizar aquellas cuestiones que resulten especialmente delicadas, como la continuidad del servicio y el factor de disponibilidad o las repercusiones en la reputación del establecimiento o servicio turístico.

ABSTRACT

This doctoral thesis focuses on the contracting of *Cloud Computing* services in its modality of public implementation by the small entrepreneur, which takes place online and through general conditions. The public *cloud* mode allows the small business owner an economic and simple implementation of computer resources, which will be received through the Internet, and in which the provider will be responsible for acquiring, maintaining and updating the computer systems that support the service. Our work aims to provide a uniform treatment of the most common contents of non-negotiated *Cloud Computing* contracts, and especially the obligations that integrate the legal relationship between the small subscriber and the service provider. On the other hand, we want to determine the legal nature that corresponds to the generality of public cloud contracts. Finally, solutions to the specific problems arising from these new and extended contracts related to the ownership of the migrated data, the protection of privacy and the destination of the remaining data in the supplier's systems are proposed, once the contract has been

ended.

Regarding the *cloud* contracts signed by the small business owner of the tourism sector, we want to identify the most popular public cloud deployment services, and analyze those issues that are especially sensitive, such as the continuity of the service and the availability factor or the impact on the reputation of the establishment or tourist service.

ÍNDICE

ASPECTOS JURÍDICO-MERCANTILES DE LA SUSCRIPCIÓN DE SERVICIOS DE COMPUTACIÓN EN LA NUBE POR PEQUEÑOS EMPRESARIOS; EN PARTICULAR, IMPLICACIONES EN EL SECTOR TURÍSTICO

VOLUMEN I

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

VOLUMEN II

ÍNDICE

ÍNDICE

ÍNDICE

INTRODUCCIÓN

Vivimos en una era altamente tecnológica, en la que estamos inmersos de forma inevitable, y en la que son pocos (tanto empresarios como particulares) quienes pueden, o quieren, prescindir de Internet. De la evolución de Internet y de su ingeniería técnica nace la computación en la nube, el fenómeno mundial que se presenta como recurso de aprovisionamiento tecnológico cada vez más habitual[1]. Entre otras funcionalidades, el usuario de servicios de nube pública puede acceder a recursos de computación desde cualquier dispositivo con conexión a Internet, y puede almacenar datos, compartirlos, editarlos, organizarlos o coordinarlos con datos de otros usuarios, puesto que se procesan, guardan y copian remotamente en equipos hardware del proveedor. Todo ello de forma económica, cómoda y rápida.

Por ello, en la actualidad, los datos se encuentran cada vez menos en ordenadores y cada vez más en gigantescos centros de procesamiento de datos

1 La Fundación del Español Urgente (Fundéu BBVA) recomienda emplear el término "computación en la nube", y no *Cloud Computing*, en informaciones sobre tecnología, de acuerdo con la *Ortografía de la Lengua Española,* donde se considera desestabilizador el uso de extranjerismos innecesarios. Fundéu BBVA es una institución que impulsa el buen uso del español en los medios de comunicación, formada por periodistas, lingüistas y lexicógrafos, y está asesorada por la Real Academia de la Lengua. Ésta última aún no ha introducido el término "computación en la nube" en su Diccionario, ni se ha pronunciado sobre la corrección de su uso. En este trabajo, sin embargo, y con el fin de evitar la continuada repetición de una única expresión, nos referiremos indistintamente a la tecnología de computación en la nube a través de diferentes expresiones, entre las que se encuentran, además de las anteriores: "la nube", "servicios en la nube", o "computación remota". Igualmente, y en favor de la simplificación, mayor agilidad en la lectura y mejor entendimiento, utilizaremos en ocasiones la palabra "*cloud*" como adjetivo referente a esta tecnología y que describirá, por ejemplo, al proveedor, cliente o contrato de servicios de computación en la nube.

externalizados, cuya ubicación, como veremos más adelante, suele ser desconocida para el usuario. La transmisión electrónica de información es imparable: la nube (metáfora que evoca la ubicación remota de la información virtual que se transmite a través de una red al hacer uso de estos servicios) se llena de secretos empresariales, de información personal, de actividades administrativas y financieras o de bases de datos que albergan conocimientos multidisciplinares[2].

A su vez, los proveedores del sector tecnológico presentan infraestructuras, plataformas, aplicaciones y otros servicios en línea que pretenden impulsar la investigación y la innovación empresarial con soluciones que se amoldan a los requerimientos de los diferentes sectores y a la envergadura y productividad de cada organización. El diseño de aplicaciones que se despliegan en dispositivos móviles permite realizar tareas prácticamente desde cualquier lugar e impulsa la productividad de sus clientes empresarios. Los proveedores compiten por lanzar herramientas cada vez más inteligentes y pueden personalizar sus productos y servicios en atención a un sector empresarial específico, o por el contrario, comercializarlos de forma masificada y con alta escalabilidad para todo tipo de público[3].

La computación en la nube se caracteriza por prestarse a modo de autoservicio, gracias a una aplicación de manejo sencillo que permite ajustar el volumen de recursos suministrado a la demanda concreta del cliente (elasticidad). La red de comunicaciones (en muchos casos, Internet) se configura como la vía de transmisión de recursos e información, utilizando el proveedor el mismo hardware para facilitar tales recursos a múltiples usuarios a la vez. El proveedor mide el uso y distribución de estos recursos entre los distintos suscriptores a través de monitorizaciones, con distintos fines: determinar la contraprestación por el servicio de acuerdo con los recursos consumidos por cada cliente, controlar que el uso del servicio sea acorde con lo contratado y que no se produzcan abusos o usos indebidos, o realizar informes y estadísticas para evaluar otros aspectos del servicio (como el rendimiento, los perfiles de la demanda, el análisis de errores o fallos, etc.).

Con estas mismas características, el suscriptor puede elegir entre cuatro

2 En realidad, esta información se aloja en servidores físicos que integran los diferentes centros de datos pertenecientes a prestadores de servicios de computación en la nube. GARCÍA SÁNCHEZ, Manuel, "Retos de la computación en la nube", *Derecho y Cloud Computing* (Coord. Ricard Martínez), 1ª edición, Navarra, 2012, págs. 39 a 40.

3 "Escalabilidad". Habilidad de un sistema o proceso para reaccionar y adaptarse a variaciones en la demanda por parte de los clientes de los servicios suministrados. (Definición propia).

diferentes modelos de implementación de sistemas de computación en la nube en su empresa y entre tres tipos de modelo de negocio. Así, como modelos de implementación, tenemos por una parte las nubes privada y comunitaria, que suelen suscribirse por unos pocos clientes en exclusiva, y por otra, la nube pública, en la cual se centra este trabajo, cuya oferta contractual se presenta para el público en general. La nube híbrida, como su propio nombre indica, integra características de la nube privada y la nube pública. En cuanto a los modelos de negocio, estos se configuran atendiendo al tipo de recursos contratados. Si se trata de recursos de hardware o red virtual, hablaremos de infraestructura como servicio (IaaS). Si se trata de herramientas y entornos para el desarrollo, la prueba y la gestión de programas informáticos, hablaremos de servicios de plataforma (PaaS). Si lo que se facilita al cliente es una aplicación informática con diferentes funcionalidades, nos referiremos al software como servicio (SaaS). Nuestro trabajo, como se verá más adelante, se centra especialmente en el modelo de implementación de nube pública.

La relevancia económica y social de la computación en la nube ha provocado que la Comisión Europea se involucre en impulsar esta tecnología. La Comunicación de la Comisión Europea titulada *Unleashing the Potential of Cloud Computing in Europe* prevé que en el año 2020, se creen gracias al Cloud Computing 2,5 millones de puestos de trabajo en Europa y unos beneficios de 160 billones de euros, lo que implicaría un aumento del producto interior bruto de un 1%[4]. Por ello, la propia Comisión creó el Grupo de Expertos en *Cloud Computing,* con tres finalidades: conseguir unas condiciones contractuales "seguras y justas"; establecer estándares que permitan la interoperabilidad, portabilidad de datos y reversibilidad; y desarrollar el *European Cloud Partnership*, un organismo de colaboración en materia de *Cloud Computing* que integre a la industria y al sector público. Si bien se han conseguido diferentes resultados gracias a los trabajos dedicados a la computación en la nube, sobre todo en materia de estandarización tecnológica y privacidad, a nuestro parecer quedan todavía materias por tratar, especialmente en ciertas cuestiones relacionadas con la contratación *online* de servicios de software, tales como la distribución equitativa de responsabilidades, la propiedad de los datos, el control y uso de los contenidos del cliente por parte del proveedor, la revelación de datos

4 Así se declara en su Comunicación *Unleashing the Potential of Cloud Computing in Europe* COM(2012) 529 final, de 27 de septiembre de 2012. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>. Para mas información, ver también el sitio web oficial de la *European Cloud Computing Strategy* de la Comisión Europea, disponible en: <https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy>. [Fecha de consulta: 3 de abril de 2017].

migrados de carácter no personal o la modificación unilateral de contenidos contractuales[5]. A nuestro parecer, y como exponemos más adelante, deberían recogerse algunas de las prácticas habituales en el mercado de servicios de *Cloud Computing* sobre estas materias como susceptibles de considerarse abusivas y de crear situaciones de falta de equidad, especialmente cuando tienen lugar en relaciones jurídicas entre proveedores *cloud* y suscriptores de estos servicios que sean pequeños empresarios y consumidores.

En el ámbito internacional, cabe destacar la tarea que está llevando a cabo el Grupo de Trabajo IV, dedicado al comercio electrónico, de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), que prepara un texto sobre los aspectos contractuales de la computación en la nube, atendiendo a la propuesta del Gobierno de Canadá titulada "Posible labor futura en materia de comercio electrónico: cuestiones jurídicas que afectan a la computación en la nube". La finalidad de este texto será "ayudar a las partes contratantes a determinar los obstáculos, las limitaciones y otras dificultades que pueden presentarse en la negociación o la ejecución de contratos de servicios de nube", con lo cual "se formulan recomendaciones con el fin de sugerir formas posibles de resolver determinadas cuestiones que pueden plantearse en relación con esos contratos". Respecto de las cuestiones que pretenden abordarse, se recogen, entre otras, aspectos sobre la autenticación de usuarios, la descripción de los servicios y los parámetros de calidad, la distribución de riesgos, cuestiones de propiedad intelectual, exenciones y

5 El Grupo de Expertos en contratos de *Cloud Computing* se creó mediante la Decisión de 18 de junio de 2013 2013/C 174/04. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:174:0006:0008:EN:PDF>. Dentro de este grupo de expertos se crearon diferentes subgrupos, siendo uno de ellos el *Cloud Select Industry Group on Code of Conduct.*, encargado de elaborar un código de conducta a seguir por los proveedores del sector Cloud a modo de buenas prácticas. Si bien las diferentes materias mencionadas (responsabilidad, modificación unilateral de cláusulas, uso de los datos del cliente por parte del proveedor, etc.) y se han redactado informes para su debate por el propio Grupo de Expertos, lo cierto es que la redacción de un código de buenas prácticas que trate tales aspectos no se ha llevado a cabo por el momento. Dichos informes están disponibles en el siguiente enlace: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. Sí se ha desarrollado por el Grupo de Expertos, en cambio, un código de conducta modelo respecto de cuestiones contractuales relacionadas con la privacidad, revisado por el Grupo de Trabajo del Artículo 29, y que actualmente se encuentra pendiente de tramitación. Más información sobre este código de conducta en privacidad para proveedores *cloud* disponible en: <https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers>. Si bien a lo largo de este trabajo se referenciarán algunos informes del Grupo de Expertos de la Cloud Computing Strategy, nos remitimos asimismo para información sobre la *European Cloud Computing Strategy* a su sitio web oficial, disponible en: <https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy>. [Fecha de consulta: 3 de abril de 2017].

limitaciones de responsabilidad, o modificación del contrato. De momento, parece que el texto resultante revestiría la forma de texto de orientación, sin carácter legislativo, cuyos beneficiarios sean los contratantes con menor poder de negociación, en el que se efectúe una distinción, por una parte, de las cuestiones propias de todos los contratos de computación en la nube, independientemente del tipo de implementación (privada, comunitaria, pública o híbrida) y del modelo de negocio (infraestructura, plataforma o software)y, por otra, de las cuestiones propias de cada tipo de contrato[6].

Por otra parte, el *Cloud Computing* también ha sido objeto de distintos trabajos por parte de organismos dedicados a la protección de datos de carácter personal, tanto a nivel europeo como nacional, como el Grupo de Trabajo del Artículo 29 o la Agencia Española de Protección de Datos[7], así como de organismos especializados en la seguridad de la información, como el Instituto Nacional de Ciberseguridad INCIBE (antes INTECO)[8].

A la vista de estos antecedentes, esta tesis doctoral se centra en la contratación de servicios de computación en la nube en su modalidad de implementación pública, por parte de pequeñas y medianas empresas (es decir, en su forma de contratación mercantil), en línea y a través de cláusulas de adhesión. Ello es así, en primer lugar, porque la opción más habitual entre profesionales y pequeños y medianos empresarios es la contratación de la modalidad pública de nube, debido a su bajo coste y facilidad de implementación en la operativa empresarial, y a que consume escasos recursos del sistema propio, quedando en manos del proveedor la

6 El Grupo de Trabajo IV de la CNUDMI sobre comercio electrónico, en su 55 sesión, que tuvo lugar en Nueva York del 24 a 28 de abril de 2017, debatió sobre los aspectos contractuales de la computación en la nube. Las cuestiones comentadas se hallan recogidas en la Nota de la Secretaria A/CN.9/WG.IV/WP.142 [en línea], págs. 5, 9 y 15. Se encuentra disponible en: <http://www.uncitral.org/uncitral/es/commission/working_groups/4Electronic_Commerce.html>. [Fecha de consulta: 30 de mayo de 2017].

7 Entre otros trabajos, cabe destacar el Dictamen 5/2012 sobre *Cloud Computing*, del Grupo de Trabajo del Artículo 29 (WP 196). Por parte de la Agencia Española de Protección de Datos, es relevante, entre otros documentos, la *Guía para clientes que contraten servicios de Cloud Computing 2013*. Disponibles en línea respectivamente en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf> y <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>. [Fecha de consulta: 3 de abril de 2017]. Ver capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

8 INTECO, *Riesgos y Amenazas en Cloud Computing* [en línea], 2011. Disponible en <http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf>. [Fecha de consulta: 3 de abril de 2017]

adquisición y el mantenimiento del hardware y del resto de sistemas que sustentan los recursos suministrados a través de Internet.

Dentro de la nube pública, la modalidad de software como servicio (SaaS) resulta la más popular y extendida, al presentar una gran diversidad de funcionalidades a modo de aplicación informática y viéndose el suscriptor liberado de realizar actualizaciones. Su uso, pensado para el público en general y la comercialización en masa, resulta sencillo y no suele precisar de amplios conocimientos informáticos. El precio suele resultar otro de los factores claves del éxito de muchos servicios de software en la nube, siendo muy reducido, e incluso, en ocasiones, substituido por otro tipo de contraprestación, no dineraria, como la cesión de derechos o de información de carácter personal, o el consentimiento a recibir publicidad no solicitada. En este trabajo, asimismo, hemos dedicado un capítulo especial al pequeño empresario turístico, que tiene a su alcance un abanico de servicios software en la nube pública especialmente diseñados para gestionar establecimientos y servicios turísticos, y destinados a solventar su problemática específica[9].

Asimismo, para aquel empresario cuyas actividades sociales están directamente relacionadas con las tecnologías de la información, como sucede con las *start-ups*, los servicios de infraestructura y plataforma implementados en la nube pública son otra opción rápida, flexible y económica para acceder a recursos virtualizados y a soluciones para el desarrollo de software.

En segundo lugar, debe puntualizarse que la contratación de la computación en nube presenta notables diferencias según el tipo de cliente. Concretamente, el objeto de este trabajo se centra en los microempresarios (de 0 a 9 empleados), pequeños (de 10 a 49 empleados) y medianos empresarios (de 50 a 249 empleados) que han suscrito o prevén suscribir este tipo de servicios para incorporarlos en su operativa empresarial. A todos ellos nos referiremos, en este trabajo, con el término

9 Este trabajo se ha realizado en el marco del proyecto DER2012-32063 «Turismo y Nuevas Tecnologías; en especial, el régimen jurídico de las denominadas centrales de reservas turísticas» (Investigadora principal: Apol·lònia Martínez Nadal) y también del proyecto DER2015-63595-R "*Big Data, Cloud Computing* y otros nuevos retos jurídicos planteados por las tecnologías emergentes; en particular, su incidencia en el sector turístico" (Investigadora principal: Apol·lònia Martínez Nadal), financiados ambos por el Ministerio de Economía y Competitividad y desarrollados en la Universitat de les Illes Balears. Además, este trabajo se ha desarrollado gracias a la ayuda de una beca otorgada por la *Conselleria d' Innovació, Recerca i Turisme del Govern de les Illes Balears* y del Fondo Social Europeo, en el marco del Programa Operativo FSE 2014-2020.

"pequeño empresario"[10]. Hemos decidido poner el punto de mira en el pequeño empresario suscriptor de servicios de computación en la nube por encontrarse, a nuestro parecer, desprotegido ante condiciones generales que pueden propiciar abusos. Ello es así, por una parte, porque no se le concede la protección de la normativa de protección a los consumidores, precisamente porque las prestaciones del contrato *cloud* se integran dentro de sus actividades comerciales y empresariales, porque carece de la suficiente fuerza contractual que le permita negociar con el proveedor en igualdad de condiciones y porque contratará, prácticamente siempre, en sede electrónica, suscribiendo las condiciones generales predispuestas por el proveedor. Por contraposición, las grandes empresas que contratan servicios de computación en la nube, cuyo suministro implica para el proveedor mayores ingresos y también mayor esfuerzo técnico (por ejemplo, la implementación de nubes privadas, comunitarias o híbridas), se encuentran en condiciones no solo de personalizar el servicio que se les suministra o de contratar modelos de implementación más exclusivos (como la nube privada o comunitaria), sino también de conseguir condiciones contractuales más favorables cuando contraten servicios de computación en la nube pública. Por ello, si bien algunas de las cuestiones aquí tratadas pueden igualmente serles extensibles, hemos decidido centrarnos en la problemática de aquel pequeño empresario que suscribe servicios de computación en la nube pública a través de condiciones generales.

Con este trabajo se persiguen distintos objetivos. Tras una primera aproximación a las características técnicas de la computación en la nube en general, a su definición y a las principales ventajas y riesgos que supone su adopción, se procederá a la determinación de la naturaleza jurídica correspondiente con la generalidad de los contratos *cloud* de nube pública. A continuación, se analizarán distintas cuestiones relacionadas con las partes del contrato y con terceros que puedan estar relacionados con esa relación contractual.

Posteriormente, se procederá a dar un tratamiento uniforme a los contenidos más comunes de los contratos *cloud* no negociados, los cuales se han sistematizado en distintos capítulos, en relación a las materias jurídicas a las cuales se refieren. Así se dedicará un capítulo a estudiar los principales aspectos jurídicos relacionados con

10 Se ha tomado como referencia para la realización de este trabajo, respecto del número de empleados que permiten identificar a una empresa como microempresa, pequeña o mediana empresa, la clasificación realizada por el Directorio General de Empresas (DIRCE) del Instituto Nacional de Estadística (INE). Para esta consideración, y a efectos de este trabajo, no se ha tenido en cuenta el volumen de negocio de la empresa.

los contenidos alojados en los sistemas remotos del proveedor, como son las responsabilidades de las partes contractuales por tales contenidos (por ejemplo, por su licitud o por el uso que se realice de estos contenidos y del servicio en general), o los aspectos relacionados con la protección que se deriva de la legislación en materia de propiedad intelectual e industrial y del secreto comercial. Se destinará otro capítulo a cuestiones relacionadas con datos de carácter personal, especialmente de aquellos tratamientos de datos de terceros que el pequeño empresario decida efectuar mediante servicios de computación en la nube. Por ello, y con vistas a la inminente aplicabilidad del nuevo Reglamento General de Protección de datos, se estudian cuestiones como la asignación de los roles de responsable, encargado y subencargado del tratamiento entre el suscriptor del servicio, el proveedor y eventuales subproveedores del servicio *cloud* y sus respectivas responsabilidades como tales, los derechos del titular de datos personales y su ejercicio en el ámbito de la computación en la nube, o la problemática derivada de la localización de los datos personales en terceros países fuera del ámbito europeo.

A continuación, se procede al estudio detallado de las diferentes obligaciones exigibles a las partes dentro de esta relación contractual, poniendo especial énfasis en aquellas que corresponden al proveedor como prestador de servicios. Así, por una parte, se procederá al estudio de aquellos compromisos relacionados con la disponibilidad del servicio, con el grado de control del proveedor sobre los recursos suministrados al cliente y con la preservación de la integridad y confidencialidad de los datos migrados. En el mismo capítulo, nos detendremos en las responsabilidades que puedan derivarse del cumplimiento deficiente de las anteriores obligaciones, de eventuales limitaciones o exenciones de responsabilidad contractualmente estipuladas y de posibles restricciones al resarcimiento del suscriptor. Dado que algunas de estas cláusulas pueden ser, a nuestro parecer, susceptibles de ser consideradas abusivas cuando el contrato de computación en la nube es suscrito por un consumidor, dedicamos un apartado a la posibilidad de la aplicación extensiva de la normativa de protección al consumidor en aquellos casos en los cuales la situación del pequeño empresario pueda asimilarse a la de aquel. Por otra parte, no nos olvidamos de las obligaciones correspondientes al cliente *cloud*, que no se restringen únicamente al pago de una contraprestación (dineraria o no) por el servicio, sino que comprenden, a nuestro parecer, otros compromisos respecto del uso del servicio.

Durante el transcurso de la relación contractual *cloud* pueden tener lugar incidencias relacionadas con la modificación de aspectos relacionados con la prestación o de las cláusulas contractuales suscritas; asimismo, pueden producirse

interrupciones o suspensiones del suministro de recursos al cliente. Todo ello por decisión unilateral del proveedor, ante la cual el pequeño empresario puede ver limitada su capacidad de reacción u oposición. Una vez se extinga el contrato *cloud* (cuyas causas y efectos también analizaremos), subsisten obligaciones del proveedor relacionadas con la recuperación de los contenidos migrados por el cliente, su portabilidad y la conservación o desaparición de réplicas de esos datos que puedan quedar remanentes servidores remotos. Las cuestiones jurídicas relacionadas con lo anterior (es decir, con la modificación, la suspensión, la extinción del contrato y el destino de los datos migrados) serán objeto de otro capítulo de este trabajo, el cual pone fin a la parte de este trabajo dedicada a los aspectos más generales de la contratación en línea de servicios de computación en la nube pública por el pequeño empresario.

Por último, el capítulo final se dedica a la utilización y a la problemática específica de los contratos *cloud* suscritos por pequeños empresarios del sector turístico. A través de sus diferentes apartados, se pretende realizar una aproximación a los servicios *cloud* más populares entre los profesionales de este sector y a aspectos que pueden serles especialmente delicados, como la continuidad del servicio y los factores de disponibilidad o las repercusiones en reputación *online* del establecimiento o servicio turístico.

Capítulo Primero

CONCEPTO Y CARACTERÍSTICAS TÉCNICAS DE LA COMPUTACIÓN EN LA NUBE

1.-INTRODUCCIÓN

Si bien el término "nube" referente a la tecnología de *Cloud Computing* resulta bastante utilizado en la actualidad, refiriéndose generalmente a aquella información transmitida y accesible a través de Internet y almacenada en servidores remotos, el concepto tanto técnico como jurídico de la prestación de servicios de computación en la nube resulta, a nuestro parecer, difuso y necesario de clarificación[1]. Algunas organizaciones internacionales especializadas (como el NIST, como veremos a continuación), han definido esta tecnología, describiéndola como el acceso bajo demanda, a través de una red de comunicaciones, a recursos informáticos (servidores virtuales, almacenamiento remoto, aplicaciones informáticas, etc.) que se suministran de manera inmediata y automatizada al cliente. Por otra parte, las

1 La Real Academia de la Lengua ha añadido, al término "nube" que figura en su Diccionario, la acepción siguiente: "Espacio de almacenamiento y procesamiento de datos y archivos ubicado en Internet, al que puede acceder el usuario desde cualquier dispositivo". A nuestro parecer, esta definición adoptada por la Real Academia se refiere al espacio virtual sin localización física determinada. Sin embargo, en las fechas de redacción de este trabajo no se encuentra recogido en el diccionario de la RAE otro término que se refiera al modo de suministro de capacidades informáticas prestado por los proveedores de computación en la nube, y que es objeto de este trabajo.

definiciones jurídicas de la computación en la nube procedentes de normativa y jurisprudencia son todavía escasas.

En este capítulo pretendemos aproximar al lector a la técnica que subyace bajo los servicios de computación en la nube (capas que integran la nube), de una manera descriptiva, a los efectos de que posteriormente pueda comprender mejor las implicaciones jurídicas de su implementación. Posteriormente haremos mención a algunas de sus principales ventajas, así como de los eventuales riesgos a los cuales se enfrenta el suscriptor de estos servicios.

A continuación, en este capítulo de aproximación al *Cloud Computing* también distinguiremos entre los distintos modelos de implementación de servicios de computación en la nube (nube privada, comunitaria, pública e híbrida), si bien el resto del trabajo se centrará en la suscripción de servicios en la nube pública, al ser los más extendidos en el sector de las PYME, por su bajo coste de suscripción y por su facilidad de implementación.

Los servicios de computación en la nube más populares para el suscriptor pequeño empresario son aquellos comercializados a modo de software como servicio (SaaS). Debido a su facilidad de uso y a no requerir especiales conocimientos técnicos informáticos para proceder a su instalación, manejo y aprovechamiento, como veremos más adelante, es con la modalidad de negocio *cloud* SaaS con la que el pequeño empresario centrado en actividades empresariales distintas a las tecnologías de la información y la comunicación suele contar de manera más frecuente[2]. Sin

2 Como veremos más adelante, los servicios comercializados de computación en la nube se organizan principalmente en tres categorías. En primer lugar, los servicios *Infrastructure as a Service* (IaaS), suministran al cliente recursos de computación (servidores, sistemas de almacenamiento, routers...), generalmente mediante la técnica de la virtualización, y este se ahorra el tener que adquirirlos e instalarlos en su propio centro de datos. Algunos de los ejemplos comerciales más conocidos son los servicios *EC2* y *S3* de *Amazon Web Services* y el servicio *SmartCloud Enterprise* de la multinacional *IBM*. En segundo lugar, si lo que buscamos es un entorno de recursos para programar, desarrollar y testear aplicaciones y demás software, la nube nos ofrece la *Platform as a Service* (PaaS), como las proveídas por las compañías *Microsoft* (*Windows Azure*) o *Google* (*Google Apps Engine*). Para acabar, debemos tener en consideración que los servicios de la nube más comercializados son, sin duda, los pertenecientes a la categoría *Software as a Service* (SaaS), cuyo contenido puede ser tan dispar como pueden serlo los programas de ordenador. Entre las muchas aplicaciones destinadas al consumidor, las más populares son las redes sociales como *Facebook* o *Twitter*, los servicios de correo electrónico con almacenaje en la nube (como *Gmail*, *Hotmail* o *YahooMail)*, o los servicios de almacenamiento remoto de información (como *Dropbox*, *SkyDrive* o *Google Drive*). En cuanto a los software como servicio destinados a las empresas, destacan las aplicaciones para administración de recursos humanos, de

embargo, otros modelos de negocio *cloud*, como los servicios de infraestructura (IaaS) o plataforma (SaaS) están a disposición de aquel empresario interesado en su suscripción cuando se adecuen a la concreta demanda de recursos computacionales del pequeño empresario cuya actividad se centre en desarrollo tecnológico o que maneje grandes cantidades de datos informáticos. Ello sucede, a modo de ejemplo, con las *start-ups* tecnológicas.

Nuestra intención es que, al finalizar este capítulo, el lector comprenda en qué consiste la prestación de servicios de computación en la nube en un sentido técnico, y pueda diferenciarlo de otros servicios similares, como el *Outsourcing* informático o el *Hosting*.

2.- ¿QUÉ ES LA COMPUTACIÓN EN LA NUBE?

Consideramos que una aproximación instrumental al concepto de la computación en la nube resulta imprescindible para la adecuada comprensión de esta nueva tecnología y, por consiguiente, de las cuestiones jurídicas que conlleva. Sin embargo, debemos mencionar de antemano que no existe unanimidad sobre a qué debemos referirnos cuando hablamos de la computación en la nube. Sirvan de ejemplo de la percepción inicial sobre el *Cloud Computing* estas palabras, a nuestro modo de ver, muy acertadas: "existe un consenso general sobre el hecho de que algo grande y profundo está pasando, aunque todavía no estemos seguros de lo que es"[3].

---

gestión de cartera de clientes, llevanza de la contabilidad y administración de recursos de la empresa, automatizaciones de procesos de venta, las interfaces para realizar proyectos de colaboración en línea, etc. Entre la soluciones de software como servicio orientados a empresas turísticas, destacan los sistemas de planificación de recursos empresariales (*Enterprise Resource Managenent* o ERP) o los sistemas de gestión de información sobre clientes (*Customer Relationship Managenent* o CRM). Muchas de estas aplicaciones se ofertan como paquetes para empresas o como servicios que estas pueden suscribir "a la carta". El proveedor es quien se ocupa de mantener el software disponible y actualizado, y de gran parte de las cuestiones de seguridad. Ver apartado "Los modelos de servicio en la nube", en este mismo capítulo, y capítulo "La contratación de servicios de computación en la nube por el pequeño empresario turístico".

3 Así describió la impresión general que suscitaba en sus inicios la computación en la nube el informe de la Fundación de la Innovación Bankinter: "*Cloud Computing. La tercera ola de las tecnologías de la información*" [en línea]. 2010, pág. 12. Disponible en: <http://www.well-comm.es/wellcommunity/wp-content/uploads/CloudComputing.pdf>. [Fecha de consulta: 30 de marzo de 2017]. Muestra de esta falta de consenso es el artículo "T*wenty-one Experts Define Cloud Computing*", publicado en la revista *Cloud Computing Journal* y en el que se pretende delimitar en qué consiste, a ojos de expertos técnicos, el fenómeno *cloud.* GEELAN, Jeremy, "T*wenty-one Experts Define Cloud Computing*" [en línea], *Cloud Computing Journal*, 2009. Disponible en: <http://cloudcomputing.sys-con.com/node/612375>. [Fecha de consulta: 30 de

No obstante lo anterior, la computación en la nube ha ido evolucionando durante estos últimos años, y ha sido objeto de diferentes definiciones que describen sus características esenciales, aunque tales definiciones no sean totalmente coincidentes[4]. Por ello, para proceder a la aproximación conceptual a la computación en la nube, acudiremos a diversas fuentes. En primer lugar, procederemos a enumerar las definiciones del término *Cloud Computing* proporcionadas por diferentes instituciones encargadas de la elaboración de estándares técnicos y tecnológicos, y, posteriormente, distinguiremos el *Cloud Computing* de otros conceptos informáticos con los cuales puede confundirse o está relacionado[5]. Posteriormente, expondremos las definiciones jurídicas aportadas por instituciones españolas, europeas e internacionales.

2.1.- Definición y características técnicas según el *National Institute of Standards and Technology* (NIST)

El *National Institute of Standards and Technology* es uno de los principales responsables del desarrollo de estándares y directrices técnicas y de seguridad en materia tecnológica y científica. Se fundó en 1901 en Estados Unidos y actualmente forma parte de su Departamento de Comercio, donde promueve la innovación y la competitividad de las industrias norteamericanas, convirtiéndose en un referente mundial dentro del sector de las tecnologías de la información y la comunicación (TIC).

En septiembre de 2011, el NIST publicó su última definición de *Cloud Computing,* que es la que sigue: "el *Cloud Computing* es un modelo para proporcionar el acceso, bajo

---

marzo de 2017].

4 Aunque en general existe un consenso sobre lo que es el *Cloud Computing*, en ciertos aspectos la coincidencia sobre lo que abarca este término no es absoluta, especialmente en lo que se refiere al software como servicio, como veremos en el apartado "Qué no es *Cloud Computing",* en este mismo capítulo.

5 La empresa *Compaq* se atribuye el mérito de acuñar el término *Cloud Computing*, en 1996, posteriormente utilizado por otras compañías como *Google* o *Amazon*. En el siguiente enlace puede verse el documento que, según parece, menciona el término *Cloud Computing* por primera vez.
<https://s3.amazonaws.com/files.technologyreview.com/p/pub/legacy/compaq_cst_1996_0.pdf>. [Fecha de consulta: 30 de marzo de 2017]. Para más información sobre el origen de este término, ver REGALADO, Antonio, "Who coined Cloud Computing?" [en línea], *Technology Review,* 2011. Disponible en: <http://www.technologyreview.com.br/printer_friendly_article.aspx?id=38987>. [Fecha de consulta: 30 de marzo de 2017].

demanda y a través de la red, a un conjunto de recursos compartidos configurables (por ejemplo: redes, servidores, almacenaje, aplicaciones y servicios) que pueden ser rápidamente suministrados y lanzados al cliente con un sencillo manejo y con mínima interacción con el proveedor. Se compone de cinco características, tres modelos de servicio y cuatro modelos de implementación"[6].

Como vemos, el NIST define el *Cloud Computing* como un modelo que proporciona acceso en respuesta a la demanda del cliente de forma rápida, utilizando una red de comunicaciones como canal de entrega, prácticamente sin interacción con el proveedor. El objeto que se proporciona consiste en recursos computacionales (tales como redes de comunicación secundarias, servidores virtuales, almacenamiento, aplicaciones y otros servicios informáticos) que, generalmente, proceden de un "contenedor" común y se compartirán entre diferentes usuarios.

Según el NIST, la computación en la nube se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación, los cuales describe en el mismo documento técnico[7]. A continuación y para una mejor comprensión del concepto técnico del *Cloud Computing*, analizaremos con detalle cada una de estas características, dejando para apartados posteriores la explicación relativa a sus diferentes modelos de implementación y servicio. Si un servicio no reúne estas características que describimos a continuación, conforme a los criterios del NIST no nos hallaremos ante un verdadero servicio de computación en la nube.

2.1.1.- Autoservicio bajo demanda

La primera característica propia de los servicios de computación en la nube es el "autoservicio bajo demanda", denominado así por el NIST[8]. Consiste en que el cliente puede proveerse por sí mismo de las capacidades contratadas (almacenamiento, servidores virtuales, aplicaciones, etc.), a través de mecanismos

6 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST; *Special Publication 800-145. The NIST definition for Cloud Computing* [en línea], 2011. Disponible en: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>. [Fecha de consulta: 24 de junio de 2016]. Traducción propia del original: "*Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model is composed of five essential characteristics, three service models, and four deployment models".*

7 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST; *Special Publication 800-145. The NIST Definition of …*, *op. cit.*, págs. 2 a 3.

8 Traducción propia del original: "*On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider".* NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.*, pág. 2.

automatizados, en el momento preciso en que los requiera, que le serán suministrados desde el llamado "contenedor de recursos compartidos", y que equivaldría a diferentes centros de datos interconectados desde los cuales se transmite la capacidad informática al cliente.

Esta cualidad permite una reducción de costes para el cliente empresario: en cuanto al factor tiempo, ya que se evitan procesos largos porque obtienen un aumento de capacidad inmediato y personalizado tras efectuarse la petición; en cuanto a esfuerzo, puesto que esta variación de capacidades tendrá lugar sin necesidad de paralizar la operativa empresarial; y en cuanto a capital humano, puesto que el diseño sencillo de la interfaz permite aumentar o disminuir el volumen de recursos sin necesidad de contar con personal informático altamente especializado en su plantilla[9].

Igualmente, esta configuración de la prestación a modo de autoservicio permite al cliente acceder a los recursos que necesita de forma ágil, sobrellevando mejor las diferentes cargas de trabajo que se le presenten en su operativa empresarial. Por ejemplo, para hacer frente al manejo de grandes cantidades de datos altamente confidenciales o críticos, puede ser preferible un elevado nivel de seguridad a una rápida velocidad de procesamiento. A su vez, los proveedores son capaces de responder eficazmente a las fluctuaciones de demanda de sus clientes prácticamente en tiempo real.

2.1.2.- Acceso a través de red

Los recursos puestos a disposición por el proveedor están disponibles en red y son accesibles a través de una red de comunicaciones, generalmente, desde cualquier dispositivo con acceso de banda ancha a Internet (ADSL, fibra óptica, satelital, etc.): teléfonos móviles, tabletas, ordenadores portátiles o de sobremesa, videoconsolas, etc[10]. Internet, pues, se configura como la vía de entrega del servicio en muchas de

9 El informe ISO 1788:2014 reconoce las ventajas que proporciona esta característica de la computación en la nube. ISO/IEC; *International Standard 1788:2014 Information technology - Cloud computing - Overview and vocabulary* [en línea], 2014, pág. 5. Disponible en: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>. [Fecha de consulta: 28 de junio de 2016].

10 Traducción propia del original: "*Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)*". NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST; *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 2. Pueden existir nubes que funcionen a través de redes internas privadas y no a través de Internet,

las nubes.

Gracias al acceso al servicio por red, el proveedor puede distribuir y mover los datos del cliente entre diferentes centros de datos geográficamente dispersos, para optimizar su rendimiento y minimizar riesgos y costes de operación. No obstante, es una de las obligaciones del proveedor *cloud* permitir el acceso a tales datos para el cliente conectado[11], aunque este desconozca su particular ubicación[12].

Actualmente, el uso del servicio se realiza a través de estándares de interfaz de servicio web, para facilitar al cliente el enlace de sus propias aplicaciones y las capacidades suministradas por el proveedor[13]. Por ejemplo, el cliente se conecta a un sitio web y accede mediante unas credenciales a los servicios o contenidos contratados. Este sistema le permitirá no tener que descargar programas o adquirir dispositivos añadidos para poder hacer uso de los servicios *cloud*, ni cargar con su instalación o actualizaciones.

2.1.3.- Agrupación de recursos y "*multi-tenancy*"

En el entorno *cloud,* los recursos físicos y virtuales que el proveedor pone a disposición de sus múltiples clientes se agrupan a modo de grandes "contenedores de recursos" o "*resource pools",* y los recursos que albergan se asignan dinámicamente a

---

como por ejemplo las nubes privadas o comunitarias *on premise*. Sin embargo, aunque posteriormente procederemos a su definición, quedan fuera del objeto de este trabajo, centrado en la contratación de servicios de nube pública.

11 Ver capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

12 De hecho, el cliente no puede controlar la localización exacta de sus datos, aunque es posible que el proveedor especifique de forma genérica dónde pueden ser transferidos o alojados (por ejemplo, el país, conjunto de países o región continental). A esto debemos añadirle que los datos no se encuentran almacenados estáticamente en un único centro de datos, sino que pueden ser transferidos a diferentes centros de datos a conveniencia del proveedor. Como veremos más adelante, puede que el proveedor del servicio con el que el cliente ha contratado tenga a su vez contratado con un tercero otro servicio (correspondiente a una capa inferior a la ofertada), y que sea este tercero quien decida sobre la localización de los datos del cliente. La pérdida, puesta en compromiso o falta de disponibilidad de los datos del cliente implicará responsabilidades que analizaremos en otros capítulos. Ver apartado "La cadena de suministros de servicios de computación en la nube", en el capítulo "Concepto y características técnicas de la computación en la nube", y apartado "Obligaciones del proveedor", en el capítulo "Contenido del contrato de computación en la nube".

13 "Interfaz". Según la RAE, "Conexión física y funcional entre dos aparatos o sistemas independientes". La acepción a la cual hacemos referencia es a la interfaz de servicio web, cuya principal función es permitir al usuario interaccionar con la aplicación o aplicaciones contratados con el proveedor *cloud,* mediante un manejo comprensible e intuitivo. Como ejemplo, el conocido estándar HTTP.

uno u otro cliente de acuerdo a las demandas de estos[14]. Por ello resulta difícil delimitar una ubicación física determinada en la cual se encuentren los recursos, ya que, a menudo, provienen de centros de datos geográficamente dispersos y se replican entre ellos por razones de disponibilidad, resiliencia y seguridad. Aun así, es posible determinar la localización de estos recursos de una manera más abstracta, por ejemplo, delimitando los países entre los cuales se mueven esos datos[15].

Los clientes del proveedor o proveedores comparten los recursos albergados en estos "contenedores"[16], gracias a la arquitectura en capas de la nube, diseñada especialmente para albergar a múltiples usuarios, característica que recibe el nombre de "multitenencia" (en inglés, *multi-tenancy*)[17]. Aunque la necesidad de interacción entre varios usuarios puede generar conflictos relacionados con la gestión del sistema y la compartición de recursos, el proveedor de cada capa garantiza un entorno protegido y aislado para cada uno de ellos mediante controles de acceso y otros mecanismos de seguridad y disgregación que hacen inaccesibles los datos de un cliente por parte de otros usuarios con quienes comparte tales recursos. Así, el proveedor debe asegurarse de que los datos y aplicaciones de cada cliente conservan su integridad y confidencialidad, y que son inaccesibles por otros clientes con los que

14 Como veremos más adelante, la nube privada se caracteriza por ser exclusiva de un único gran cliente, con lo cual carece de la multitenencia o compartición de los recursos con otros usuarios.

15 El NIST describe así la multitenencia: *"The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth"*. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 2.

16 En las nubes privadas, sin embargo, no se produce esta compartición de recursos, puesto que se crean para uso exclusivo de un único cliente. Ver apartado "Los modelos de implementación de la computación en la nube".

17 La nube se estructura internamente en capas o niveles de servicio: la capa hardware corresponde al propio centro de datos físico y a los recursos materiales tangibles que soportan las capas lógicas (servidores, *routers*, sistemas de encendido y refrigeración, etc.); la capa de infraestructura crea el contenedor de recursos lógicos a través de la virtualización; el nivel de plataforma, que contiene sistemas operativos para desarrollar software y ofrecer soporte a la interfaz de la aplicación de la nube; y la capa de aplicación, que consiste en las propias aplicaciones que ofrece la nube (redes sociales, servicios web, aplicaciones empresariales...). Cada una de estas capas puede implementarse como servicio para dar soporte a su capa superior, dando lugar a tres diferentes modelos de negocio: IaaS, PaaS y SaaS. Ver apartado "Las capas que integran la nube y su tecnología subyacente", en este mismo capítulo.

se comparte el hardware[18].

Los recursos que se ofrecen en forma de provisión de servicio son infinitamente variados, y, como hemos comentado, pueden abarcar, entre otros, potencia de procesamiento, ancho de banda o espacio de almacenaje, o plataformas de programación informática o aplicaciones de software más o menos complejas[19].

2.1.4.- Rápida elasticidad

La nube proporciona una manera elástica de abastecerse de las capacidades de computación y permite liberar las que no se usan, generalmente de forma automática y mediante el autoservicio, ajustándose a las necesidades de demanda existentes en cada momento[20]. Así se optimiza al máximo el uso de los recursos, evitando que se abastezcan en exceso o se desaprovechen, y facilitando la máxima escalabilidad hacia los recursos que requiere cada cliente.

Esta elasticidad y la consiguiente escalabilidad de los recursos computacionales resultan idóneas para entornos informáticos y de desarrollo de aplicaciones complejas, cuya demanda de recursos puede variar de forma amplia y rápida[21]. La asignación dinámica y automatizada de recursos se consigue mediante evaluaciones constantes de las fluctuaciones de la demanda, realizadas por el propio sistema *cloud* del proveedor, y no únicamente en los momentos con picos de cargas de trabajo. Se retornan al "contenedor" los excedentes para que otros usuarios puedan hacer uso de ellos. Esta facultad de aprovisionamiento (y desaprovisionamiento) está siempre disponible para el cliente sin procesos largos, ya que tiene lugar de forma inmediata y automatizada.

A menudo, el proveedor oferta la flexibilidad al cliente como la capacidad de disponer de recursos de computación "ilimitados", ya que el usuario puede acceder a

18 Integridad y confidencialidad son dos aspectos de la seguridad de los datos albergados en la nube, como se verá en el apartado "riesgos técnicos", en este mismo capítulo.

19 Ver capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube

20 Traducción propia del original en inglés: "*Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time*". NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition…, op. cit.,* pág. 2.

21 "Escalabilidad". Sistema o proceso diseñado para reaccionar y adaptarse a cambios en la demanda de capacidad, gestionando el crecimiento progresivo de trabajo de manera continuada y sin pérdida de calidad en su funcionamiento. (Definición propia).

ellos en cualquier volumen e instantáneamente, y como hemos mencionado, sin necesidad alguna de adquisición o mantenimiento de hardware o instalación de software accesorio. Así, el cliente puede acceder a los recursos que necesita atendiendo a sus picos de demanda, y sujetándose únicamente a eventuales límites que vengan determinados contractualmente por el proveedor.

2.1.5.- Sujeción a métrica y monitorizaciones

Es muy frecuente que los sistemas de computación en la nube monitoricen o controlen la utilización que hacen los usuarios de los recursos, más si se tiene en cuenta que múltiples servicios *cloud* se retribuyen en función del uso de esos recursos o del número de usuarios que acceden a ellos. Estos controles se llevan a cabo mediante herramientas específicas de software que proporciona el propio proveedor, aunque el cliente puede utilizar mediciones de terceros si lo considera adecuado[22].

Las monitorizaciones del uso que hacen los clientes del servicio tendrán su relevancia jurídica, por un lado, en cuanto a la determinación de la remuneración del servicio por parte del cliente y en cuanto al cumplimiento del nivel de servicio contratado, y por otro lado, en relación a ciertos derechos del usuario respecto de los controles ejercidos sobre las actividades que lleva a cabo al utilizar los servicios[23].

Del mismo modo, también puede medirse el uso y distribución de los recursos suministrados a los clientes con la finalidad de recopilar información sobre el rendimiento de las aplicaciones, posibles intervalos de inactividad, detección de errores del sistema y sus causas, eventuales fallos de seguridad, control de accesos a información almacenada, etc. Dado que estos controles aportarán transparencia

22 El NIST describe así las monitorizaciones: "*Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service*". NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 2.

23 En relación a este último aspecto, consideramos que el cliente tiene derecho a ser informado de la existencia de tales auditorías, tanto en su papel de responsable del tratamiento de datos personales de terceros como si de estas se pudiera desprender la suspensión del servicio por decisión unilateral del proveedor. Las auditorías reflejarán el efectivo cumplimiento de ciertas cláusulas contractuales, en concreto las referidas a los requisitos mínimos del nivel del servicio que debe suministrar el proveedor (ANS) y a la política de uso adecuado (PUA) con la que el cliente se compromete a utilizar de forma legal y leal los recursos facilitados. Ver capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

sobre el efectivo consumo de recursos y la calidad de su prestación, sus resultados podrán aprovecharse en la toma de decisiones sobre la gestión de recursos y operativa empresarial, tanto por el proveedor como por el cliente.

Una vez analizadas las características derivadas del concepto de *Cloud Computing* definido por el NIST, cabe destacar la especial relevancia de esta definición, dado que ha sido adoptada como referente por diferentes instituciones europeas, como el Grupo de Trabajo del Artículo 29 y la propia Comisión Europea[24].

2.2.- Otras definiciones técnicas

A continuación, nos detendremos en las definiciones técnicas del *Cloud Computing* aportadas por otros organismos relevantes.

2.2.1.- Definición por el *American National Standards Institute* (ANSI)

Otro de los referentes en cuanto a la supervisión del desarrollo de estándares para productos, servicios, procesos y sistemas es el *American National Standards Institute.* Se trata de una organización no lucrativa norteamericana que forma parte de la Organización Internacional para la Estandarización (*International Organization for Standardization,* ISO) y que promueve la estandarización de normas de productos y seguridad para empresas y organizaciones a nivel nacional y su posterior coordinación internacional, conocidas como "normas ISO"[25]. El establecimiento de

24 El Grupo de Trabajo del Artículo 29 es un órgano consultivo independiente formado por representantes de las Autoridades de Protección de Datos de cada uno de los Estados miembros. Sus principales funciones incluyen el estudio de cuestiones relacionadas con la aplicación de las disposiciones de la Directiva, emitir dictámenes sobre el nivel de protección existente en los Estados miembros y en terceros países, asesorar a la Comisión Europea y realizar recomendaciones en materia de protección de datos. Fue creado por la Directiva 94/46/CE del Parlamento Europeo y del Consejo 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. Sirvan de ejemplo de la adopción de la definición de computación en la nube el *Dictamen 5/2012 sobre la computación en la nube* del Grupo de Trabajo del Artículo 29 (WP 196) de 1 de julio de 2012 (págs. 4 a 5), y la Comunicación de la Comisión Europea titulada *Unleashing the potential of Cloud Computing in Europe,* COM (2012) 529 final, de 27 de septiembre de 2012 (pág. 3). Disponibles respectivamente en los siguientes enlaces: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf> y <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>. [Fecha de consulta: 30 de marzo de 2017].

25 El equivalente español del *American National Standard Institute* es la Asociación Española de Normalización y Certificación (AENOR), una entidad privada sin ánimo de lucro creada en 1986, con presencia en todas las Comunidades Autónomas y en otros países. La norma ISO 17788:2014

este tipo de estándares es fundamental para una eficaz transferencia internacional de tecnologías y su óptimo funcionamiento global[26].

La norma ISO/IEC 17788:2014 define diferentes conceptos relacionados con este entorno tecnológico, como sus características principales, y los relaciona y desarrolla para presentar una visión en conjunto del contexto *cloud*.

Este documento define el *Cloud Computing* como "entorno que facilita acceso a través de una red a contenedores de recursos físicos o virtuales, de manera elástica y escalable, que se proporciona a modo de autoservicio y bajo demanda"[27]. La norma se fundamenta en la definición aportada por el NIST, y pone también como ejemplo de recursos informáticos servidores, sistemas operativos, redes, software, aplicaciones o sistemas de almacenamiento.

Esta definición es, a nuestro modo de ver, clara en cuanto a los aspectos técnicos esenciales que comparten todos los servicios de computación en la nube.

---

tiene en España una norma muy similar, denominada UNE 71380/2014. Hemos destacado la organización americana y no la española porque el grupo de trabajo que se encarga específicamente de desarrollar estándares en el campo de distribución de plataformas y servicios de aplicaciones (dentro del cual se integra la tecnología de computación remota) depende del secretariado americano ANSI.

26 La IEC es otra organización destinada a preparar y publicar estándares internacionales para cualquier tecnología eléctrica, electrónica o relacionada con estas. Se creó en 1906 y tiene divisiones en diferentes países. Suele trabajar en cooperación con expertos del ISO y la ITU (*International Telecomunication Union*) para asegurarse de que los estándares elaborados son compatibles y se complementan adecuadamente. Los grupos de trabajo mixtos entre estas organizaciones aseguran que los estándares internacionales combinan los conocimientos principales que convergen entre las áreas tecnológica, electrónica y de telecomunicaciones. Además de estas, existen otras asociaciones que desarrollan sus estándares, como la *IEEE Standards Association*, que dedica dos grupos de trabajo a desarrollar estándares de perfiles de nube e interconexión entre nubes. Dentro del *Joint Technical Comitee* (JTC) de la ISO y la *International Electrotechnical Commission* (IEC) se formaron tres grupos de trabajo en octubre de 2009, cuyo objetivo era la "*Standardization for Interoperable Distributed Application Platforms and Services*". Para alcanzar este objetivo resultó necesario proporcionar la definición, terminología y requisitos de estandarización del *Cloud Computing*, de cuyo desarrollo se encargó el Grupo de Trabajo 3, denominado ISO/IEC JTC 1/SC 38/WG3. La norma ISO/IEC 17788:2014, uno de los resultados del trabajo de este grupo, define el concepto de *Cloud Computing* y de otros vocablos relacionados con esta tecnología informática. Otra norma ISO relevante es la ISO 27018:2014, que establece criterios orientadores para proveedores de servicios *cloud r*especto de controles adecuados de seguridad de la información de carácter personal.

27 Traducción propia del original en inglés: *"Paradigm for enabling network access to scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand"*. CLOUD SECURITY ALLIANCE, *Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1* [en línea], 2009. Disponible en: <https://cloudsecurityalliance.org/csaguide.pdf>. [Fecha de consulta: 30 de marzo de 2017].

2.2.2.- Definición por la Cloud Security Alliance (CSA)

La *Cloud Security Alliance* es una organización norteamericana nacida en 2008, sin ánimo de lucro, que promueve el uso de buenas prácticas en cuestiones de seguridad dentro del *Cloud Computing*, y participa al desarrollo de estándares técnicos, en colaboración con otras instituciones. Está integrada por compañías proveedoras, asociaciones y otros miembros del sector tecnológico y de la computación en la nube.

Su definición de *Cloud Computing* es la que sigue: "La computación en nube es un concepto en evolución que describe el desarrollo de varías tecnologías existentes y convierte el acceso a recursos computacionales en algo diferente. La nube separa las aplicaciones y los recursos informáticos de la infraestructura subyacente y de los medios utilizados para su provisión. (…) La nube describe la utilización de una miscelánea de servicios, aplicaciones, datos e infraestructura integrados en contenedores de recursos de computación, red, datos y almacenaje. Estos recursos pueden sincronizarse, suministrarse, implementarse y darse de baja de forma inmediata, y sus dimensiones son ajustables. Se proporcionan en forma de suministro, bajo demanda y atendiendo a las necesidades de consumo"[28].

La CSA es consciente de la multitud de definiciones que intentan abordar la nube desde diferentes perspectivas, y remarca que la definición que facilita se dirige a profesionales de la seguridad de las Tecnologías de la Información. Reconoce y toma como referencia la definición aportada por el NIST, para "aportar coherencia y consenso en cuanto a la adopción de un lenguaje común"[29], aunque afirma que la elección de la definición elaborada por el NIST como modelo de referencia "no excluye otros puntos de vista de nacionalidades diferentes a la nortemericana"[30].

Como puede observarse, tanto de esta definición aportada por la *Cloud Security Alliance* como de las anteriores referenciadas en este trabajo, pueden extraerse similitudes que evidencian en qué consiste el *Cloud Computing*[31]. Podemos

---

28 Traducción propia del original: "*Cloud Computing is an evolving term that describes the development of many existing technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them. (…) Cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources. These components can be rapidly orchestrated, provisioned, implemented and decommissioned, and scaled up or down; providing for an on-demand utility-like model of allocation and consumption".* CLOUD SECURITY ALLIANCE, *Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1* [en línea], 2009. Disponible en: <https://cloudsecurityalliance.org/csaguide.pdf>. [Fecha de consulta: 30 de marzo de 2017].

29 Cloud Security Alliance, *Security Guidance for …, op.* cit, pág. 14.

30 Cloud Security Alliance, *Security Guidance for …, op.* cit, pág. 14.

31 Queremos remarcar que únicamente hemos aportado aquellas definiciones técnicas que, a nuestro

concluir, sin duda alguna, que la computación en la nube se distingue por proporcionar acceso inmediato a recursos informáticos de diferente índole (aplicaciones informáticas, almacenamiento de contenidos digitales, capacidad de procesamiento, etc.) a través de una interfaz de usuario puesta a disposición por el proveedor y de manejo sencillo, y que estos recursos se suministrarán al cliente por medio de una red de comunicaciones, de manera automatizada y ajustable a su demanda.

Puesto que estas características propias de la computación en la nube se complementan con otros términos y descripciones recogidos en el documento elaborado por el NIST relativo a la definición de la computación en la nube, en especial los referentes a las capas que integran esta tecnología y sus modelos de implementación y servicio, más adelante nos detendremos en su análisis.

2.3.- Qué no es *Cloud Computing*

El uso del término *Cloud Computing* se ha popularizado, y con él, la confusión con otras tecnologías y servicios que coexisten en el mercado. Para centrar el objeto de este trabajo, dedicamos este apartado a distinguir la tecnología de la computación en la nube de otros conceptos técnicos que, si bien no coinciden exactamente con la definición aportada por el NIST, pueden estar relacionados con la computación en la nube o compartir algunas de sus características. Concretamente, nos referiremos brevemente al llamado *Grid Computing*, al modelo de *Utility Computing*, a la virtualización, al *Outsourcing*, al *Hosting* y a la Web 2.0.

2.3.1.-*Grid Computing* o computación en malla

El *Grid Computing* es una infraestructura informática que permite a diferentes instituciones (empresas, centros de investigación, universidades, etc.) la compartición de recursos (procesamiento, almacenamiento, aplicaciones, etc.) y la administración conjunta de sistemas informáticos de alto rendimiento para lograr una meta concreta en cuanto al tratamiento de información[32]. En el *Grid Computing*,

parecer, consideramos de mayor relevancia, con el fin de ayudar a delimitar en qué consiste esta tecnología. Sin embargo, ello no significa que no existan otras aportaciones conceptuales igualmente válidas, aunque, por motivos de extensión, no se hayan aportado en este trabajo.

32 ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf; "Cloud Computing: State-of-the-art and Research Challenges" [en línea], *Brazilian Computer Society*, 2010, pág. 8. Disponible en: <http://link.springer.com/article/10.1007%2Fs13174-010-0007-6>. [Fecha de consulta: 30 de marzo de 2017].

los recursos de distintos sistemas informáticos se utilizan de forma conjunta, generalmente para resolver un concreto problema a gran escala que requiere de gran capacidad de procesamiento[33].

La computación en la nube comparte ciertos aspectos con el *Grid Computing*[34]. Los dispositivos informáticos de la computación en malla están interconectados e integrados a través de computación distribuida, como sucede en el *Cloud Computing*: el hardware se encuentra distribuido en diferentes localizaciones físicas, aunque su conexión a través de una red de telecomunicaciones permite que los diferentes centros de procesamiento funcionen como una único equipo, con lo cual pueden reducirse inversiones en infraestructura y aumentarse la capacidad de carga de los sistemas. Ambas tecnologías permiten la escalabilidad, que se consigue gracias a la distribución de cargas de trabajo que se ejecutan de manera separada entre los diferentes nodos interconectados en red, y al aprovisionamiento de capacidades de procesamiento, ancho de banda y almacenamiento. Del mismo modo, las dos tecnologías permiten la realización de diferentes tareas por múltiples usuarios de los mismos recursos, los cuales se comparten, aumentando la eficiencia y la gestión de picos de trabajo, y reduciendo la inversión en tiempo de procesamiento. Ello es así porque la computación en malla, en combinación con otras tecnologías, permitió la consolidación y la expansión del concepto actual de computación en la nube[35].

No obstante lo anterior, la computación en la nube va más allá, al virtualizar tecnologías en diferentes niveles (infraestructura, plataforma y software), permitiendo el aprovisionamiento dinámico a través de redes de comunicaciones como Internet[36]. En el *Grid Computing*, los recursos se activan o desactivan, pero no

33 Un ejemplo de utilización de *Grid Computing* es el *SETI Home Project*. Esta institución sin ánimo de lucro (*Search for Extra-Terrestrial Intelligence*), fundada en 1984 y que realiza distintos proyectos científicos para la búsqueda de vida extraterrestre inteligente, diseñó un programa que se ejecuta en el ordenador del usuario conectado a Internet y facilita tareas de procesamiento de datos obtenidos por radiotelescopios. Más información en su sitio web, disponible en: <http://setiathome.ssl.berkeley.edu/>. [Fecha de consulta: 30 de marzo de 2017].

34 MYERSON, Judith; *Cloud Computing versus Grid Computing* [en línea], 2009, pág. 3. Disponible en: <http://www.ibm.com/developerworks/library/wa-cloudgrid/>. [Fecha de consulta: 30 de marzo de 2017].

35 *"In fact, the Cloud Computing is built on top of several other technologies, for example Distributed Computing, Grid Computing, and Utility Computing"*. SCHAWISH, Ahmed; SALAMA, Maria; "Cloud Computing. Paradigms and Technologies", *Springer Studies in Computational Intelligence 495*, Berlín, 2014, pág. 40.

36 ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf, *op. cit,* pág. 8.

se produce lo que venimos denominando aprovisionamiento bajo demanda. El *Cloud Computing*, a diferencia del *Grid*, puede considerarse una *Utility Computing*, como veremos a continuación, ampliando su funcionalidad no solo para soportar altas cargas de trabajo de grandes empresas e instituciones, sino facilitando un volumen menor de recursos a un mayor número de usuarios, como pequeños empresarios y consumidores.

2.3.2.- *Utility Computing*

La *Utility Computing* no es una tecnología en sí misma, sino un concepto que representa el modelo de provisión de recursos de computación bajo demanda y tarifables por consumo[37]. El término "*utility*" aplicado al *Cloud Computing* indica que, a través de esta tecnología, se suministran recursos de computación de manera similar a otros recursos como la electricidad o la telefonía, a modo de servicios. Se trata de un modelo de comercialización que permite optimizar el uso de los recursos y reducir al máximo los precios, todo ello organizado en torno a la idea de consumo según demanda y prestación de servicios, en contraposición a la inversión en activos tecnológicos que tenía lugar tradicionalmente.

Sin embargo, la computación en la nube implica mucho más que el modo de comercialización de la informática antes expuesto, puesto que combina tecnologías existentes para proporcionar diferentes tipos de recursos al cliente, desvinculando el acceso a los recursos informáticos de la adquisición y mantenimiento de dispositivos físicos. A su vez, los recursos de computación pueden comercializarse a modo de *Utility Computing* sin necesidad de basarse en entornos de *Cloud Computing,* por ejemplo, un sistema informático que suministra recursos a clientes y carece de virtualización[38]. Por estas razones, no pueden considerarse equivalentes ambos términos.

2.3.3.- Virtualización

37 BROBERG, James; VENUGOPAL, Srikumar; BUYYA, Rajkumar; "Market-oriented Grids and Utility Computing: The State-of-the-art and Future Directions", *Journal of Grid Computing,* 2008, Vol. 6, núm. 3, págs. 255 a 276. ARMBRUST, Michael; FOX, Armando [et al]; *Above the Clouds: a Berckeley View of Cloud Computing* [en línea], 2009, pág. 4. Disponible en: <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>. [Fecha de consulta: 30 de marzo de 2017].

38 BISWAS, Sourya; *Cloud Computing vs. Utility Computing vs. Grid Computing. Sorting the diferences* [en línea], 2011. Disponible en: <http://cloudtweaks.com/2011/02/cloud-computing-vs-utility-computing-vs-grid-computing-sorting-the-differences/>. [Fecha de consulta: 30 de marzo de 2017].

Nos referimos a la virtualización, como hemos observado anteriormente en este capítulo, para hablar de una técnica informática que, a través de software específico, aísla las funcionalidades del hardware físico y crea versiones virtuales de diferentes recursos tecnológicos. La virtualización es la técnica que permite al *Cloud Computing* separar la capa de hardware de las capas superiores, agrupar los recursos en "contenedores", y asignarlos y distribuirlos entre los diferentes clientes atendiendo a su demanda[39]. Aunque generalmente se entiende por virtualización la partición virtual de un servidor físico en múltiples servidores virtuales, realmente esta técnica se aplica a otros recursos, como almacenamiento, redes, sistemas operativos o aplicaciones[40].

Así, la virtualización es un elemento esencial de los entornos en la nube, con lo cual están estrechamente relacionados. Sin embargo, no son conceptos intercambiables, ya que la virtualización no conlleva algunos de los aspectos característicos de la computación en la nube, como el autoservicio o la elasticidad. En otras palabras, la computación en la nube es la prestación, a través de Internet y bajo demanda, de servicios resultantes de la virtualización, pero no toda virtualización implica la prestación de servicios de computación en la nube.

2.3.4.- *Outsourcing*

Por otro lado, la computación en la nube podría considerarse una mera modalidad del *Outsourcing* tradicional[41]. Se ha definido el *Outsourcing* de sistemas informáticos como "la técnica de gestión empresarial consistente en la externalización, total o parcial, de las necesidades o tareas informáticas que con anterioridad venían siendo desarrolladas en el seno de la propia organización (o podrían haberlo sido), por un período largo de tiempo (generalmente entre 5 y 10 años), a

39 ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf, *op. cit.*, pág. 9.

40 La virtualización de servidores consigue que las cargas de trabajo se consoliden en un número más reducido de servidores plenamente utilizados. La virtualización de almacenamiento permite albergar volúmenes de datos a gran escala, frágmentándolos, y posteriormente se reagrupan y se entregan al cliente cuando los reclama. La virtualización de red permite crear redes más elásticas y con mayor capacidad, así como redes virtuales privadas independientes y seguras. La virtualización de sistemas operativos permite alojar en un mismo dispositivo sistemas operativos independientes sin interferencias. La virtualización de aplicaciones permite trabajar con aplicaciones que no se instalan (al menos, completamente) en el sistema del cliente, sino que se acceden en línea. HON, W. Kuan; MILLARD, C, "Cloud Technologies and Services", *Cloud Computing Law,* (Coord. Christopher Millard), 1ª edición, Oxford, 2013, págs. 6 a 8.

41 HON, W. Kuan; MILLARD, C, "Control, Security, and Risk in the Cloud", *Cloud Computing Law,* Oxford, 2013, pág. 29.

cambio de un precio, fijado en relación a diferentes criterios"[42].

Aunque tanto el *Outsourcing* como la computación en la nube pueden considerarse técnicas de gestión de activos informáticos, la diferencia fundamental entre ambas es que en los servicios *cloud* no se contrata a un tercero para que procese los datos y lleve a cabo la gestión de un centro de datos de una empresa, sino que los datos los procesa el propio cliente, a modo de autoservicio, empleando la infraestructura y los recursos que el proveedor le suministra. Además, en el *Outsourcing* no se comparten entornos entre diferentes clientes, sino que se trata de un servicio a medida, con lo cual quienes procesan los datos deben tener elevados conocimientos técnicos, a diferencia del usuario de nube, quien generalmente procesará sus propios datos a través de interfaces sencillas, con lo cual suele ser suficiente con unos mínimos conocimientos informáticos.

Como podemos observar, la diferencia entre ambos conceptos técnicos no es radical, puesto que algunas trazas del *Outsourcing* pueden ser predicables de nubes privadas para grandes clientes. Sin embargo, los caracteres del *Outsourcing* no se adecuan a entornos de nube pública masivamente comercializables ni a las definiciones de la mayoría de software como servicio. Carece de muchas de las características esenciales de la nube, como la escalabilidad y elasticidad automática, el autoservicio, la multitenencia, el acceso a recursos virtuales a través de la red y la reducción en la inversión en infraestructura informática, como se verá en posteriores apartados. A diferencia de la nube pública, que ofrece unas prestaciones estandarizadas a las cuales el cliente debe adaptarse, el *Outsourcing* necesariamente precisa de personalización de la gestión. Por ello, no se comercializa bajo condiciones generales de contratación a las que se adhieren consumidores y pequeñas empresas, sino mediante contratos negociados altamente detallados y adaptados a las concretas necesidades y requisitos de la empresa cliente. Según el análisis realizado por APARICIO VAQUERO "no cabe hablar de Outsourcing con consumidores" puesto que "es una técnica de gestión empresarial extremadamente compleja y delicada", con "necesidad de prestar una gran atención a los tratos preliminares o a la fase prenegocial", dentro de una "relación basada

42 APARICIO VAQUERO, Juan Pablo; *La nueva contratación informática. Introducción al Outsourcing de los sistemas de información,* 1ª edición, Granada, 2002, pág. 23. Según la sentencia del Tribunal Supremo de 24 de octubre de 1994, en la que se dirime un conflicto entre la multinacional IBM y su filial IBM ISS, el *Outsourcing* informático consiste en la prestación por un tercero (en este caso, la filial) de "servicios de configuración, desarrollo, gestión y explotación de sistemas de información basados en las técnicas de la información".

en la confianza"[43].

En capítulos posteriores, abordaremos cómo estas divergencias técnicas redundan en la distinta naturaleza jurídica de los contratos de *Outsourcing* y computación en la nube[44].

2.3.5.- *Hosting* o alojamiento web

El *Hosting* implica el almacenamiento remoto de texto, imágenes, vídeo, interfaces, aplicaciones, páginas web, archivos, etc. en servidores del proveedor, accesibles a través de Internet. El *Hosting* tradicional carece de las características elasticidad, escalabilidad, y autoservicio que posee la computación en la nube, y se asemeja más a un alquiler de espacio virtual que no se retribuye por uso, sino por espacio contratado. Gracias a la tecnología de computación en la nube, se han comercializado servicios de alojamiento web en servidores virtuales que permiten almacenar datos y realizan las mismas funciones que el *Hosting* tradicional, lo cual en ocasiones suscita dudas sobre si se trata o no de un servicio de computación en la nube[45].

En comparación con el *Cloud Computing,* ambas técnicas poseen la capacidad de albergar información del cliente (texto, imágenes, vídeo, interfaces, aplicaciones, páginas web, etc.) dentro de servidores remotos accesibles en todo momento a través de Internet. Aun así, cabe destacar que los servicios clásicos de *Hosting* se basan en una arquitectura técnica diferente a la arquitectura *cloud*. El *Cloud Computing* supera el anterior concepto, y crea, a través de centros de datos interconectados y la eventual participación de subproveedores que faciliten capas subyacentes, contenedores de recursos que permiten aumentos de capacidad inmediatos y

43 APARICIO VAQUERO, Juan Pablo; *La nueva contratación informática..., op. cit.*, pág. 33.

44 Ver apartado "Figuras afines al contrato de computación en la nube", en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

45 De hecho, existen los llamados servicios de *Cloud Hosting*, una especie de *Hosting* compartido entre diferentes clientes aunque con las características de escalabilidad y tarifa por consumo de recursos más propias de entornos *cloud,* servicios que nosotros nos inclinamos a calificar como servicios de *Cloud Computing*, sin perjuicio de un análisis detallado en cada caso del contenido contractual concreto. Pueden pertenecer a las categorías de infraestructura como servicio (IaaS) o plataforma como servicio (PaaS). En el primer caso, se proporciona el servidor a modo de máquina virtual, sobre el cual poder instalar el software que el cliente escoja. Con la plataforma como servicio, el cliente recibe la plataforma software como un paquete completo que soporta el desarrollo de aplicaciones web.

adaptables a la demanda de sus múltiples usuarios, así como el replicado de datos. Gracias a la arquitectura en capas, la asignación bajo demanda de estos recursos a los clientes se produce de manera dinámica.

Como se ha podido observar, existe cierta similitud entre el servicio de *Hosting* y los servicios *cloud* de infraestructura como servicio que suministran unidades virtuales de almacenamiento. La diferencia principal reside en las características elasticidad y flexibilidad de los recursos que ofrece la arquitectura de la computación en la nube, y de las cuales carece el *Hosting*. Como se verá a lo largo de este capítulo, la modalidad de negocio de infraestructura como servicio no se restringe a la virtualización de almacenamiento o procesamiento, sino que puede incluir la virtualización de redes, sistemas operativos o aplicaciones, (además de otras características que complementan a la virtualización), las cuales quedarían fuera del ámbito del *Hosting*.

En capítulos posteriores, nos detendremos en las similitudes y diferencias de carácter jurídico que se derivan de los contratos de *Hosting* y computación en la nube[46].

2.3.6.- Web 2.0

La evolución de las páginas web ha llegado a confluir con la computación en la nube, especialmente respecto al disfrute de funcionalidades de software diverso que se prestan a través del acceso a sitios web, sin que el ordenador o dispositivo del usuario tenga que soportar la carga de procesamiento o actualización de ese software ni de almacenar toda la información generada por el usuario al utilizarlo.

Si la llamada Web 1.0 únicamente permitía al internauta leer contenidos publicados en el sitio web, este concepto se superó con la Web 2.0, al aprovecharse las ventajas de Internet para desarrollar un mecanismo de colaboración entre usuarios y sitios web, creando contenidos interactivos[47]. Los caracteres que definen a la Web 2.0 son su asimilación a un servicio que permite economías de escala, en contraposición con el software empaquetado tradicional; que se enriquece cuanto más usuarios lo utilizan; que confía en los usuarios como desarrolladores de

46 Ver apartado "Figuras afines al contrato de computación en la nube", en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

47 Ejemplos conocidos del concepto de Web 2.0 previo a la aparición de la computación en la nube podrían ser *Wikipedia*, *Youtube* o *TripAdvisor*.

contenidos; que facilita su uso autónomo por el cliente y sin necesidad de ser auxiliado por el proveedor o de necesitar elevados conocimientos técnicos; y que utiliza interfaces sencillas para conseguir lo anterior[48].

El uso de la Web 2.0 como plataforma para crear y compartir contenidos se considera como un concepto anterior al *Cloud Computing*, y por ello, en muchas ocasiones, no puede considerarse a la Web 2.0 como un servicio susceptible de ser prestado a un cliente, sino que únicamente nos encontramos ante sitios web que permiten la participación colaborativa y el uso en abierto para cualquier persona. La actual convergencia de la Web 2.0 con la tecnología *cloud* supone que, especialmente en los software como servicio (SaaS), sea complicado en ocasiones distinguir entre ambas, como se verá más adelante, puesto que ambas tecnologías se fusionan en la práctica, y encontrándonos literatura contradictoria respecto a tal diferenciación, especialmente en lo referente a redes sociales y servicios de correo electrónico[49].

En nuestra opinión, y coincidiendo con algunos autores, la Web 2.0 primitiva es uno de los múltiples elementos tecnológicos que ayudaron a crear los cimientos de los actuales servicios de computación en la nube[50]. Asimismo, la fusión de ambas tecnologías y la evolución de la Web 2.0 desde que se combina con la arquitectura en

48 O'REILLY, Tom; "What is Web 2.0: Design Patterns and Business Models for the next generation of Software", *Communications & Strategies*, núm. 65, 2007, pág. 37.

49 Por ejemplo, autores como Simon Bradshaw, Ian Walden y Christopher Millard, de la *Queen Mary University of London*, o Michael Gordon y Kathreen Marchesini, de la University of North Carolina, consideran a las redes sociales y al correo electrónico como software como servicio, y, por tanto, servicios de computación en la nube. Del mismo modo, la norma ISO-IEC 17788:2014 considera las comunicaciones como servicio (es decir, correo electrónico y redes sociales) una "categoría de servicio *cloud* en la cual la capacidad provista al cliente es interacción y colaboración en tiempo real" (traducción propia). Sin embargo, Michael Armbrust y Armando Fox, de la Universidad de Berkeley, consideran que las redes sociales son servicios diferentes a la computación en la nube, aunque se sirven de ella como tecnología de soporte. BRADSHAW, Simon; MILLARD, Christopher; WALDEN, IAN; "Standard contracts for Cloud Computing Services", *Cloud Computing Law,* 1ª edición, Oxford, 2013, pág. 41. GORDON, Michael; MARCHESINI, Kathryn; *Examples of Cloud Computing Services* [en línea], 2010. Disponible en: <https://www.unc.edu/courses/2010spring/law/357c/001/cloudcomputing/examples.html>. [Fecha de consulta: 30 de marzo de 2017]. ARMBRUST, Michael; FOX, Armando [et al], *op. cit,* pág. 8.

50 "*We can track the roots of clouds computing by observing the advancement of several technologies, especially in hardware (virtualization, multi-core chips), Internet technologies (Web services, service-oriented architectures, Web 2.0), distributed computing (clusters, grids), and systems management (autonomic computing, data center automation)*". VOORSLUYS, William; BROBERG, James; BUYYA, Rajkumar, "Introduction to Cloud Computing", *Cloud Computing Principles and Paradigms* (Coord. Rajkumar Buyya, James Broberg, Andrzej Goscinski), 1ª edición, New Jersey, 2011, pág. 5.

capas propia de la computación en la nube tiene como resultado que las funcionalidades de algunas Webs 2.0 sean susceptibles de ser prestadas a modo de servicios de computación en la nube, con lo cual resulta dificultoso en ocasiones deslindar donde acaba la Web 2.0 y donde empieza el software como servicio, especialmente respecto de aquellas que no requieren al usuario que los remunere mediante una contraprestación monetaria. De entre estas funcionalidades, destacamos las siguientes categorías, a título de ejemplo y como lista abierta: comunicación social[51], compartición de información[52], almacenamiento de contenidos[53], edición colaborativa[54], marcado y organización de enlaces y archivos en línea (también llamados marcadores sociales)[55]; etc.

Dicho lo anterior, a nuestro parecer existirían indicios que permiten considerar a algunas Web 2.0 como un modelo de negocio *cloud* de software como servicio. Por ejemplo, el hecho de que exijan autenticación al usuario para que este pueda acceder a la aplicación web, que impliquen el almacenamiento remoto de datos creados o migrados por el usuario, que la implementación del pago por el uso de la aplicación sea razonable, que presente las características de escalabilidad y elasticidad propias de la nube, que permitan un cierto grado de personalización por el cliente, que impliquen la suscripción de condiciones generales, que ofrezcan aplicaciones algo complejas y potentes, etc.

No pretendemos realizar una delimitación más precisa entre ambos conceptos desde la perspectiva técnica debido a su dificultad, tal y como evidencian las mencionadas discusiones del sector técnico al respecto. Ello no impide, sin embargo, que nos decantemos por la adopción de una solución práctica en cuanto a la inclusión de algunas Web 2.0 en el objeto de este trabajo, que incluye el análisis de condiciones generales que se suscriben por pequeños empresarios para poder proceder al uso de aplicaciones informáticas que se prestan a modo de servicio. Así, hemos optado por adoptar un concepto amplio de software como servicio de computación en la nube, que incluye redes sociales, correo electrónico y otras aplicaciones que impliquen el almacenamiento remoto de información.

---

51 Por ejemplo, blogs de participación abierta (es decir, no solo de lectura) y redes sociales como *Facebook*, *Twitter* o *Linkedin,* o servicios de correo electrónico como *Gmail* o *Hotmail*.

52 Por ejemplo, *Youtube*.

53 Por ejemplo, *Box* o *Dropbox*.

54 Por ejemplo, *Google Docs*, *Microsof Office 365* o *Zoho*.

55 Ejemplos de marcadores sociales son *Delicious* o *Evernote*. Permiten organizar y almacenar por categorías o etiquetas enlaces web y poderlos recuperar posteriormente.

Como argumento a favor de nuestra postura, ha de mencionarse que la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales (COM (2015) 634 final), asimila el suministro de contenidos digitales a la puesta a disposición del cliente a través de Internet, tal y como tiene lugar en entornos de computación en la nube: *"«suministro»: hecho de facilitar el acceso a contenidos digitales o poner a disposición los contenidos digitales".* Por ello puede entenderse que esta Propuesta de Directiva acoge el sentido amplio del software como servicio, ya que, dentro del concepto de "contenidos digitales" se integran múltiples contenidos y funcionalidades digitales, como la compartición de archivos o la interacción con datos facilitados por otros usuarios: "art. 2.1: «contenido digital»: a) datos producidos y suministrados en formato digital, por ejemplo vídeo, audio, aplicaciones, juegos digitales y otro tipo de software, b) servicio que permite la creación, el tratamiento o el almacenamiento de los datos en formato digital, cuando dichos datos sean facilitados por el consumidor, y c) servicio que permite compartir y cualquier otro tipo de interacción con datos en formato digital facilitados por otros usuarios del servicio" [56].

Todos estos servicios son susceptibles de ser suscritos por pequeños empresarios, quienes se verán afectados por muchas de las cuestiones jurídicas y aspectos contractuales propios del *Cloud Computing*, como aquellos relacionados con el almacenamiento remoto y la recuperación de datos, la deslocalización de la información, la protección de datos personales y la distribución de responsabilidades entre usuario y proveedor. Los pequeños empresarios, como veremos, quedarían fuera de la protección de la Propuesta de Directiva de suministro de contenidos digitales, en caso de que esta llegue a aprobarse.

Podemos decir, como conclusión a este apartado sobre el concepto técnico de la computación en la nube, que la razón principal de la diferente percepción de la computación en la nube es que no se trata de una tecnología completamente nueva, sino que es el resultado de la integración de tecnologías ya existentes, que permite acceder a recursos informáticos de una manera diferente a la tradicional al desvincularse infraestructura, plataforma y software y al suministrarse a través de Internet. Gracias a esta combinación de tecnologías, la computación en la nube

56 Los contratos de computación en la nube jugaron un papel particularmente importante en la identificación de los problemas contractuales relevantes para la mencionada Propuesta de Directiva. Estas cuestiones, que fueron debatidas en profundidad por el Grupo de Expertos en Contratos de la *Cloud Computing Strategy* (del cual hablaremos más adelante), estaban relacionadas con la calidad, la responsabilidad o la modificación de los contratos. Así se reconoce en los documentos de trabajo de la propia Propuesta de Directiva, concretamente al explicarse la obtención de asesoramiento técnico para su redacción.

consigue una mejor adaptación a la demanda de tecnología informática de cada concreto usuario, la reducción de costes y la posibilidad de acceder a los recursos remotamente, entre otras ventajas[57].

3.- LA ARQUITECTURA EN CAPAS DE LA COMPUTACIÓN EN LA NUBE Y SUS PRINCIPALES MODELOS DE NEGOCIO: IAAS (INFRAESTRUCTURA COMO SERVICIO), PAAS (PLATAFORMA COMO SERVICIO) Y SAAS (SOFTWARE COMO SERVICIO)

La ingeniería interna de la computación en la nube, creada de forma modular mediante capas, sustenta un conjunto de servicios ofertables relacionados con las funciones de las distintas capas que integran su arquitectura[58].

Existen tres capas lógicas que se despliegan a partir del hardware físico o capa física del proveedor, formada por centros de procesamiento de datos, conexiones y otros artefactos de su equipo informático. Estas capas reciben los nombres de capa de infraestructura, capa de plataforma y capa de aplicación, y junto con el hardware físico que las sustenta, forman las cuatro capas de la arquitectura en la nube[59].

Cada una de estas capas genera capacidades o cualidades informáticas que pueden comercializarse, gracias a esta ingeniería interna, a modo de recursos a los cuales accede el cliente. Así, la capa de infraestructura informática proporciona los recursos informáticos de procesamiento, almacenamiento o red. Del mismo modo, la capa de plataforma permite al cliente el acceso a entornos que le permitan desarrollar, administrar y ejecutar aplicaciones informáticas, pudiendo utilizar para ello diferentes lenguajes y herramientas de programación. Por último, la capa de software posibilita al cliente el uso de aplicaciones informáticas del proveedor[60]. Todos estos recursos, al ser accesibles por el cliente a través de Internet de manera

57 ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf*, op. cit.*, pág. 8.

58 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 2.

59 La opinión extendida es que la nube únicamente consta de las tres capas lógicas, aunque según algunos autores, con los que coincidimos, no puede obviarse la capa hardware, puesto que sirve de sustento físico a éstas. ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf, *op. cit.*, pág. 9.

60 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 2.

escalable, mensurable, bajo demanda, y "multi-teniente"[61], integran respectivamente los llamados modelos de negocio o de servicio *cloud*: la infraestructura como servicio (*Infraestructure as a Service* o IaaS), la plataforma como servicio (*Platform as a Service* o PaaS) y el software como servicio (*Software as a Service* o SaaS).

Sin embargo, como veremos, la arquitectura en capas de la nube es compleja, y la prestación del servicio al cliente puede depender de otros servicios proporcionados por terceros, que suministran las funciones relativas a capas subyacentes[62]. Funciones, por tanto, que pueden ser subcontratadas por el proveedor que presta el servicio al cliente final[63]. A menudo, el cliente desconocerá de la existencia de estas subcontrataciones, ya que el servicio aparentemente se presta al cliente con apariencia de independencia. Por tanto, la característica modularidad en capas de la computación en la nube permite la entrada en el mercado de múltiples proveedores y puede implicar cadenas de subcontrataciones entre las cuales a menudo se diluyen las obligaciones y responsabilidades[64].

A continuación, explicaremos con más detalle cual es la función de cada una de estas capas.

3.1.- Las capas que integran la nube y su tecnología subyacente

Como hemos mencionado, la arquitectura de la computación en la nube puede dividirse, en términos generales, en cuatro capas o niveles: la capa de hardware, la capa de infraestructura, la capa de plataforma y la capa de software[65].

3.1.1.- La capa de hardware

La capa de hardware contiene los recursos tangibles que soportan la nube y que integran uno o varios centros de datos. Forma una estructura de dispositivos informáticos integrada por servidores físicos, *routers*, cableado, sistemas de

61 De acuerdo con las características esenciales de la tecnología de la computación en la nube descritas por la definición del NIST.

62 HON, W. Kuan; MILLARD, C, *Cloud Technologies..., op. cit.*, págs. 13 a 16.

63 Por ejemplo, el software como servicio *Dropbox* se sirve de recursos de infraestructura que le proporciona otro proveedor: Amazon. Aunque recientemente esta información está disponible en su página web, tiempo atrás el cliente que contrataba con *Dropbox* no sabía que parte de su servicio dependía de la infraestructura de otro proveedor.

64 Ver capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

65 ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf*, op. cit.,* págs. 9 y 10.

encendido y refrigeración, paneles de control, componentes de redes de telecomunicaciones y demás elementos que sirven de soporte físico para el resto de capas, de contenido lógico.

3.1.2.- La capa de infraestructura

La capa de infraestructura crea contenedores de recursos informáticos a través de la virtualización, una tecnología fundamental para el desarrollo de la computación en la nube[66]. La virtualización realiza particiones de recursos físicos, dando lugar a máquinas virtuales o *virtual machines* (VM).

Aunque existen diferentes métodos de virtualización, el resultado final es la escisión entre los recursos físicos y los computacionales, permitiendo a los usuarios concentrarse en las acciones y no en la administración y mantenimiento de los equipos técnicos[67]. Los múltiples usuarios, como hemos mencionado anteriormente, comparten el uso de una infraestructura física común (servidores, procesadores, memoria e interfaces) y mediante las máquinas virtuales se benefician de una utilización mucho más económica y eficiente que con la adquisición de máquinas propias. Los usuarios permanecen aislados unos de otros mediante herramientas de software, sin separadores físicos. Sin embargo, algunos proveedores ofrecen servicios con hardware independiente para usuarios especialmente preocupados por razones de seguridad o cumplimiento normativo que lo así lo prefieran[68]. A pesar de su evidente funcionalidad, no todas las nubes requieren el uso de máquinas virtuales, aunque sí la virtualización entendida como abstracción de la parte informática lógica (a la cual accede al cliente) de los recursos físicos (controlados por el proveedor o por terceros subproveedores), puesto que gracias a ella es posible la asignación dinámica de recursos[69].

3.1.3.- La capa de plataforma

66 Aunque existen nubes que no utilizan máquinas virtuales sino físicas (ver este mismo apartado, *in fine*), algunos aspectos clave del *Cloud Computing* solo pueden tener lugar a través de técnicas de virtualización, puesto que, como recordaremos, la virtualización puede realizarse sobre otros recursos (almacenamiento, aplicaciones, redes, etc.). Es lo que sucede, por ejemplo, con la asignación dinámica de recursos.

67 Por ejemplo, la virtualización de servidores, de redes, de sistemas operativos, etc.

68 Es el caso de la *Hybrid Cloud* de la empresa *iWeb,*o la *Elastic Compute Cloud (EC2)* de *Amazon.*

69 Algunas nubes implican lo contrario, y acoplan varios ordenadores físicos para que trabajen de forma conjunta mediante operaciones de procesado. Las usan organizaciones que manejan gran cantidad de datos, como *Facebook* o *eBay*.

La capa de plataforma, situada conceptualmente sobre la capa de infraestructura, proporciona un entorno para la programación que generalmente incluye sistemas operativos, interfaces de programación y librerías de desarrollo de aplicaciones[70]. La función principal de esta capa es minimizar la carga operativa que supone desarrollar, probar y ejecutar aplicaciones directamente sobre el hardware físico (que dispone de capacidad limitada), para suministrarlos al usuario (quien suele ser un programador informático) en línea, de forma escalable e inmediata[71]. Así, los usuarios/programadores no dependen de adquirir o mantener hardware y software específico, ni tienen que administrar otros recursos subyacentes, sino que pueden centrar su actividad en el desarrollo de los códigos de programación de sus propias aplicaciones[72].

3.1.4.- La capa de software

La capa de software contiene aplicaciones completamente desarrolladas y probadas, listas para ejecutarse y ser accesibles desde cualquier dispositivo con conexión a Internet[73]. Estas aplicaciones comparten las características de la

70 HON, W. Kuan; MILLARD, C, *Cloud Technologies ..., op. cit.*, pág. 12.

71 ZHANG, Qj; CHENG, Lu; BOUTABA, Raouf, *op. cit.*, pág. 9. Por ejemplo, la plataforma como servicio *Google App Engine* opera en esta capa para implementar almacenaje, bases de datos y aspectos lógicos utilizados para el desarrollo de aplicaciones web.

72 Cuando el usuario ya ha desarrollado el código dentro de esta plataforma, la aplicación resultante puede ejecutarse vía Internet, por ejemplo, como software como servicio (SaaS). KUAN HON, W; MILLARD, C, *Cloud Technologies ..., op. cit.*, pág. 12. Ver apartado "La arquitectura en capas de la computación en la nube y sus modelos de negocio: SaaS o Software como Servicio", en este mismo capítulo.

73 La denominación como capa de software, aunque es la más extendida, a nuestro modo de ver, no es la más precisa. El término "software" engloba no solo aplicaciones, sino también sistemas operativos, programas informáticos y otras herramientas lógicas, algunas de las cuales no son comercializables a gran escala, entre otras razones, por su complejidad técnica, por estar configuradas para funcionar con equipos hardware concretos o por estar diseñadas para realizar tareas de mantenimiento. Para nosotros, coincidiendo con otros autores, la denominación más apropiada sería "capa de aplicaciones", puesto que una aplicación informática se caracteriza por ser un programa informático diseñado como herramienta y que permite al usuario realizar una o varias tareas de forma automatizada (como procesadores de textos o suites de correo electrónico). Lo mismo sucede con la denominación del modelo de servicio *Software as a Service* o software como servicio, donde además de lo mencionado anteriormente, resulta que todos los servicios de la nube incluyen, de una u otra forma, la entrega de software como parte del servicio, ya sea para monitorizar rendimientos, desarrollar programas o implementar medidas de seguridad. No obstante, para evitar confusión al lector, utilizaremos las expresiones más generalizadas, es decir, "software como servicio", al hacer referencia a estos conceptos. HURWITZ, Judith; KAUFMAN, Marcia; HALPER, Fern, *Cloud Services for Dummies. IBM Limited Edition,* 1ª edición, New Jersey, 2012, pág. 14.

computación en la nube, como la escalabilidad automática para lograr el máximo rendimiento y la mayor disponibilidad al menor coste de operación[74]. El usuario, por su parte, no controla la configuración de la red, los servidores, el sistema operativo u otras características de la aplicación o de su soporte lógico, sino que simplemente disfruta de las funcionalidades que ofrece esa aplicación informática.

3.2.- Los modelos de servicio de la nube

La computación en la nube como modelo de negocio se identifica con la puesta a disposición del cliente de recursos calificados como "*as a Service"* o "como servicio", que se basan en un aprovisionamiento mucho más económico que la adquisición de productos y licencias para equipar un sistema informático propio con un rendimiento equivalente[75]. Cada modelo o categoría de servicio se corresponde, como hemos mencionado, con las aptitudes de la capa técnica de la nube con su mismo nombre. Así puede observarse en esta figura[76]:

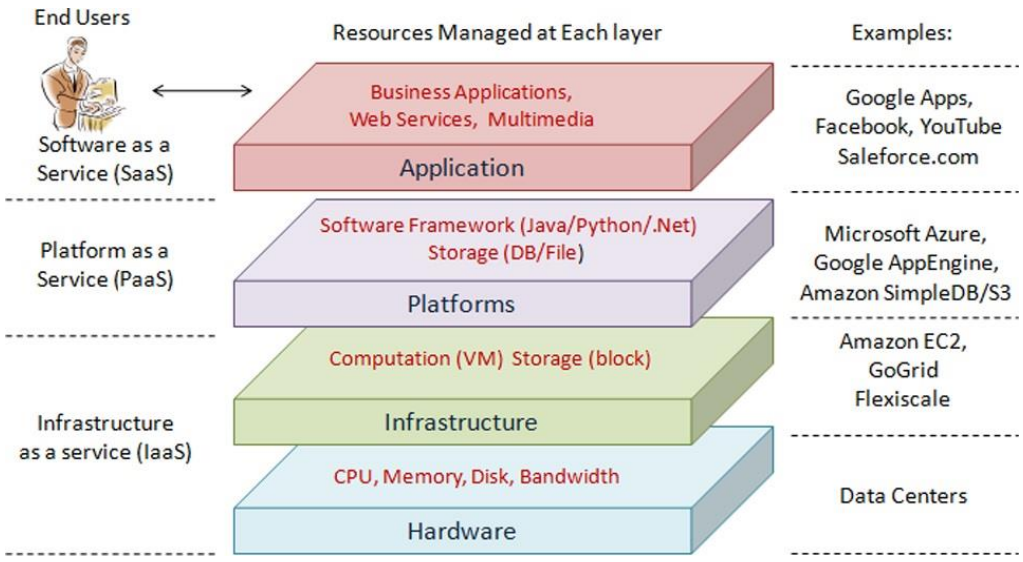

Figura nº 1. Arquitectura de la computación en la nube.

Atendiendo a las definiciones del NIST, la computación en la nube ofrece tres modelos de negocio: infraestructura como servicio (IaaS), plataforma como servicio

74 ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf*, op. cit.*, pág. 9. Ver apartado "Definición y características técnicas según el *National institute of Standards and Technology*", en este mismo capítulo.

75 HON, W. Kuan; MILLARD, C, *Cloud Technologies and Services, op. cit.*, pág. 4.

76 Figura nº 1. Fuente: ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf, *op. cit.*, pág. 9.

(PaaS) y software como servicio (SaaS), aunque cabe decir que en la práctica las diferencias entre las tres categorías no son siempre tan obvias, puesto que los proveedores cada vez ofertan servicios más complejos y ofrecen recursos procedentes de diferentes capas[77].

3.2.1.- La infraestructura como servicio (*Infrastructure as a Service* o IaaS)

El NIST define la infraestructura como servicio con estos términos: "*al usuario se le suministran las capacidades de procesamiento, almacenaje, red y otros recursos de computación esenciales, que puede utilizar para implementar y ejecutar cualquier tipo software, incluyendo sistemas operativos y aplicaciones. El usuario no administra ni controla la infraestructura subyacente de la nube, pero sí los sistemas operativos, el almacenaje y las aplicaciones que ejecuta, así como ciertos componentes de red (como los cortafuegos)*"[78].

Los recursos obtenidos pertenecen mayoritariamente a la capa de infraestructura, generalmente a modo de máquinas virtuales (virtualizaciones de servidores y demás hardware), espacio de almacenaje, ancho de banda y servicios de soporte. Puesto que es el usuario quien decide sobre el sistema operativo y el software que ejecuta dentro de los recursos que le proporciona el proveedor, correrán a su cargo la gestión de algunos aspectos de seguridad[79]. Esta gestión

---

77 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 6.

78 El documento del NIST define así la infraestructura como servicio: *"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)"* (traducción propia). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …,op. cit.,* pág. 6. [Nota a la traducción: hemos traducido el concepto anglosajón "*consumer"* como "usuario", para no causar confusión con el término "consumidor" en el sentido jurídico que le otorga el Real Decreto Legislativo 1/2007 que aprueba el texto refundido de la Ley General para la Defensa de Consumidores y Usuarios y otras leyes complementarias. En el artículo 2 de esta norma, se excluye del concepto "consumidor o usuario" a aquellos destinatarios finales que actúan en el ámbito de su actividad empresarial o profesional. En cambio, el sentido del término "*consumer"* que comprende la definición del NIST, puede perfectamente corresponder a una empresa, profesional, administración, particular o cualquier otra entidad u organismo público o privado suscriptor de un suministro de servicios de computación en la nube, sea o no destinatario final de tales servicios. También "*consumer"* podría identificarse como "cliente", en contraposición al proveedor de servicios *cloud* que le provee el suministro. El NIST es un organismo especializado en técnica informática y no en materia jurídica, por ello consideramos que su definición no tiene que analizarse con las mismas exigencias terminológicas que las definiciones legales, puesto que estas últimas son elaboradas por expertos en conceptos estrictamente jurídico-teóricos].

79 Entendiendo la seguridad como protección de activos tangibles (hardware, bases de datos...) e

concurre con la del proveedor, que es quien, en principio, se responsabiliza por el hardware y las instalaciones que lo contienen[80]. Es más, este servicio es el que ofrece al usuario un mayor control y flexibilidad sobre la configuración de la infraestructura, al contrario de lo que sucede con los servicios de plataforma o software[81].

En este modelo, el proveedor de recursos de infraestructura es el encargado de gestionar tales recursos, que se presentan como objetos virtuales accesibles a través de una interfaz, a modo de servicio bajo demanda. El cliente, no obstante, al contratar estos servicios, tiene cierto margen de maniobra para configurar aspectos del recurso, como el sistema operativo o la gestión interna de máquinas virtuales.

En vez de invertir en sus propios centros de datos, el cliente puede igualmente instalar los sistemas operativos y el software que elija dentro de la infraestructura alquilada al proveedor. Con ello consigue, por una parte, economizar en compras de hardware y en personal que lo gestione y mantenga; y por otra, la optimización máxima de los recursos de los que se dispone. A menudo, el pago se realiza por uso de los recursos consumidos, que puede efectuarse por hora o por megabyte, aunque algunos proveedores ofertan periodos de prueba del servicio gratuitos[82].

3.2.2.- La plataforma como servicio (*Platform as a Service* o *PaaS*)

Debemos tener presente la importancia de los desarrolladores de software dentro de cualquier sector empresarial, incluido el sector turístico, demandante de software y aplicaciones especializados que, por ejemplo, permitan la máxima comunicación entre el empleado y el turista. Los programadores serán los usuarios mayoritarios de los servicios en la nube de plataforma. Según el NIST, con la plataforma como servicio, "se ofrece al usuario la capacidad de desplegar, dentro de la infraestructura de computación en la nube, aplicaciones creadas o adquiridas por el propio usuario, utilizando lenguajes de programación, librerías, servicios y herramientas proporcionadas por el proveedor. El usuario no administra ni controla la infraestructura subyacente (red, servidores, sistemas operativos o almacenaje), pero tiene el control sobre las aplicaciones implementadas y sobre la configuración de algunos aspectos del entorno de desarrollo y

---

intangibles (contenido de la información almacenada o en tránsito, propiedad intelectual e industrial, etc.).

80 Como hemos mencionado, el proveedor puede, a su vez, haber subcontratado con un tercero propietario del hardware o que se encargue de su mantenimiento.

81 KUAN HON, W; MILLARD, C, "Control, Security, ...", *op. cit.*, pág. 27.

82 Como proveedores de infraestructura como servicio (IaaS), podemos mencionar Rackspace, los servicios *EC2* de Amazon Web Services, GoGrid o el servicio *Compute Engine* de Google.

hosting"[83].

Con la plataforma como servicio (PaaS) se suministra al suscriptor un entorno que comprende elementos hardware y software necesarios para el diseño, desarrollo, despliegue, testado, hospedaje y mantenimiento de aplicaciones u otras categorías de software. De esta manera, al tener todos los recursos disponibles en un único sistema y no en diferente software de múltiples terceros, se reducen para el usuario los costes de compra, mantenimiento, almacenaje y control de los elementos que integran una plataforma completa de programación. Además, el hecho de que se ofrezca como servicio en la nube facilita la homogeneización de plataformas entre colaboradores de diferentes localizaciones geográficas, el uso de versiones del código actualizadas, la implementación de estándares y el uso de entornos con capacidades elásticas y escalables[84].

El grado de control del usuario sobre las aplicaciones y la configuración del entorno de seguridad dependerá mucho de las características concretas del servicio contratado. Al igual que sucede en la infraestructura como servicio (IaaS), la seguridad se comparte entre el proveedor y el cliente. Sin embargo, y por la propia configuración del servicio y por el tipo de recursos suministrado, generalmente el usuario de servicios de plataforma dispondrá de menor capacidad de configuración sobre los aspectos relacionados con la seguridad que la que pueda disponer el usuario de servicios de infraestructura.

3.2.3.- El software como servicio (*Software as a Service* o *SaaS*)

El NIST define el software como servicio así: "*el proveedor suministra al usuario una aplicación para que este pueda desplegarla dentro de la infraestructura de computación en la nube. Las aplicaciones son accesibles desde diferentes dispositivos del cliente a través de una sencilla interfaz, facilitada por un navegador (como el e-mail con base en una web) o por la propia aplicación. El usuario no controla la infraestructura subyacente (red, servidores, sistema operativo, almacenaje) ni las características de la aplicación, excepto algunos casos en los que sí se permite configurar determinados aspectos específicamente a cada*

83 El documento del NIST define así la plataforma como servicio: *"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment"* (traducción propia.). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …,op. cit.,* pág. 6.

84 Como ejemplos de plataformas como servicio, podemos mencionar: *App Engine* de Google, *Windows Azure* de Microsoft o *Force.com* de Salesforce.com.

usuario"[85].

Como puede observarse, el usuario que suscribe este servicio está recibiendo las funcionalidades de una aplicación informática, sin necesidad de realizar cambios o actualizaciones en su equipo. Además, puede acceder al uso de la aplicación prácticamente de inmediato porque se suministra a través de la Red, y, a menudo, se le permite probar la aplicación durante un período determinado antes de proceder a su pago. En otras ocasiones, la suscripción a estas aplicaciones se ofertará sin contraprestación económica por parte del cliente[86]. Igualmente, este servicio posibilita el acceso del usuario a vastos recursos computacionales a través de dispositivos sencillos y con limitada capacidad de procesamiento y almacenaje, como teléfonos móviles o tabletas.

Una de las claves del éxito del software como servicio es que su utilización no precisa de elevados conocimientos técnicos[87]. El proveedor es quien maneja la operativa y se encarga del mantenimiento y soporte de los recursos subyacentes de la aplicación (hardware, software y redes), gracias a los cuales se proporciona el servicio[88]. Por su parte, el usuario únicamente suele tener acceso a ciertos aspectos preconfigurados de la administración, a modo de preferencias, pero su capacidad para personalizar la aplicación resulta, por lo general, muy limitada, y carece de control sobre los recursos subyacentes[89]. Así, a diferencia de lo que sucede con los servicios de infraestructura y plataforma, en el software como servicio es el proveedor el encargado de la seguridad del sistema. Aun así, el usuario deberá

85 El documento del NIST define así el software como servicio: "*The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings"* (traducción propia). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 6.

86 Ello no significa que sean servicios gratuitos, en el sentido jurídico del término, sino que la contraprestación es de contenido no dinerario. Ver apartado sobre onerosidad en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

87 INSTITUTO NACIONAL DE CIBERSEGURIDAD INCIBE (antes INTECO), *Riesgos y Amenazas en Cloud Computing* [en línea], 2011. Disponible en: <http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf>. [Fecha de consulta: 27 de junio de 2016].

88 En ocasiones, como se ha dicho, algunos proveedores de software como servicio basan sus servicios en los servicios de infraestructura o plataforma de otros proveedores. Ver capítulo "Elementos subjetivos del contrato de servicios de computación en la nube".

89 KUAN HON, W; MILLARD, C, *Cloud Technologies and ..., op. cit.*, pág. 13.

responsabilizarse de la custodia de las claves de identidad u otros mecanismos de autentificación o acceso, al ser elementos de seguridad que escapan al control del proveedor.

Otra ventaja del software como servicio es que su precio generalmente será más económico que ejecutar el software en el propio equipo del usuario, porque el proveedor puede establecer economías de escala según se vaya distribuyendo el servicio. En la práctica, algunas aplicaciones se ejecutan prácticamente sin costes para el proveedor cuando se despliegan en la nube, como aquellas que tienen millones de usuarios realizando exactamente las mismas operaciones, porque el proveedor puede optimizar los componentes del centro de datos para soportar uno o dos tipos de cargas de trabajo, dentro de una infraestructura que permita el replicado masivo[90].

El software como servicio es el modelo más popular, extendido y comercializado de los modelos de negocio de la computación en la nube. Se dirige a un mercado mucho más amplio: sus funcionalidades son útiles tanto a particulares como a empresas de todas las dimensiones o a instituciones públicas. Por este motivo, se convertirán en el prototipo de servicio *cloud* por excelencia que suscriben pequeñas empresas, y en el que centramos principalmente este trabajo de investigación y, entre ellas, las pequeñas empresas dedicadas al sector turístico.

Los servicios de software en la nube son tan variados como pueden serlo las aplicaciones informáticas[91]. Por otra parte, existen herramientas que suministran recursos relacionados con la primera capa, aunque su sencillo manejo y su escaso margen para la configuración hacen que se presten a modo de servicio de software. Concretamente, nos referimos al software como servicio de almacenamiento, conocido también como almacenamiento como servicio (*Storage as a Service)*, que provee al usuario de la infraestructura y el software para el manejo, organización y

90 HURWITZ, Judith; BLOOR, Robin; KAUFMAN, Marcia*, op. cit.*, pág. 14.

91 Por ejemplo, existen *suites* de escritorio en la nube, que en vez de instalarse en el ordenador de cada usuario permiten procesar los datos a través de Internet, como es el caso de *Microsoft Office 365.* Otros de los software como servicio con más éxito son los servicios de correo electrónico, como *Yahoo!Mail* o *Gmail*, que permiten liberar al usuario de almacenar los mensajes en su equipo, además de estar permanentemente actualizados; o las redes sociales como *Facebook* o *Twitter*, ampliamente suscritas por consumidores y empresas, que las utilizan a modo de herramientas de información y comunicación.

recuperación de datos desde cualquier lugar con conexión a Internet[92].

En cuanto a software como servicio especialmente orientado a empresas, existen desde aplicaciones aisladas de gestión de carteras de clientes[93] o de colaboración para PYME[94] hasta completos software a medida para realizar gran parte de la operativa empresarial de grandes firmas, llamados "*Business Process as a Service*". Asimismo, son muchas las empresas que utilizan software como servicio dirigido comercialmente al mercado de particulares, con propósitos empresariales[95].

Para una mejor comprensión del alcance y diferencias entre los diferentes modelos de servicio de la computación en la nube, así como de la distribución a modo general de las responsabilidades de los aspectos técnicos entre proveedor y cliente de servicios *cloud* de nube pública, facilitamos esta figura[96]:

92 A diferencia del suministro de almacenaje de la infraestructura como servicio, en el *Storage as a Service* es el mismo usuario quien gestiona el recurso, que se presenta para una moderada cantidad de datos y se promociona para atender las necesidades del consumidor o de pequeñas empresas. En cambio, el servicio de infraestructura es más adecuado para macrocantidades de datos, o datos que requieran de procesamiento especial, muy alta velocidad de transmisión, actualización y sincronización en tiempo real o unas extraordinarias medidas de seguridad. Como ejemplos, *Dropbox, Google Drive* o *Box*.

93 Como *Insightly*, o *Sales Cloud* de *Saleforce.com.*

94 Como *Google G-suite*, *Trello* o *Hangouts*.

95 Es habitual ver como empresas utilizan aplicaciones como *Facebook* a modo de Intranet gratuita, o para comunicarse con sus clientes. No obstante, la propia empresa es quien debe valorar los riesgos que puede suponer en relación a los datos que se transmiten y publican, y del uso que terceros puedan hacer de esos datos.

96 Fuente de la figura: YUNG SHOW, *Cloud Computing for IT Pros (2/6): What Is Cloud* [en línea], 2010. Disponible en: <https://blogs.technet.microsoft.com/yungchou/2010/12/17/cloud-computing-for-it-pros-26-what-is-cloud/>. [Fecha de consulta: 8 de julio de 2016].

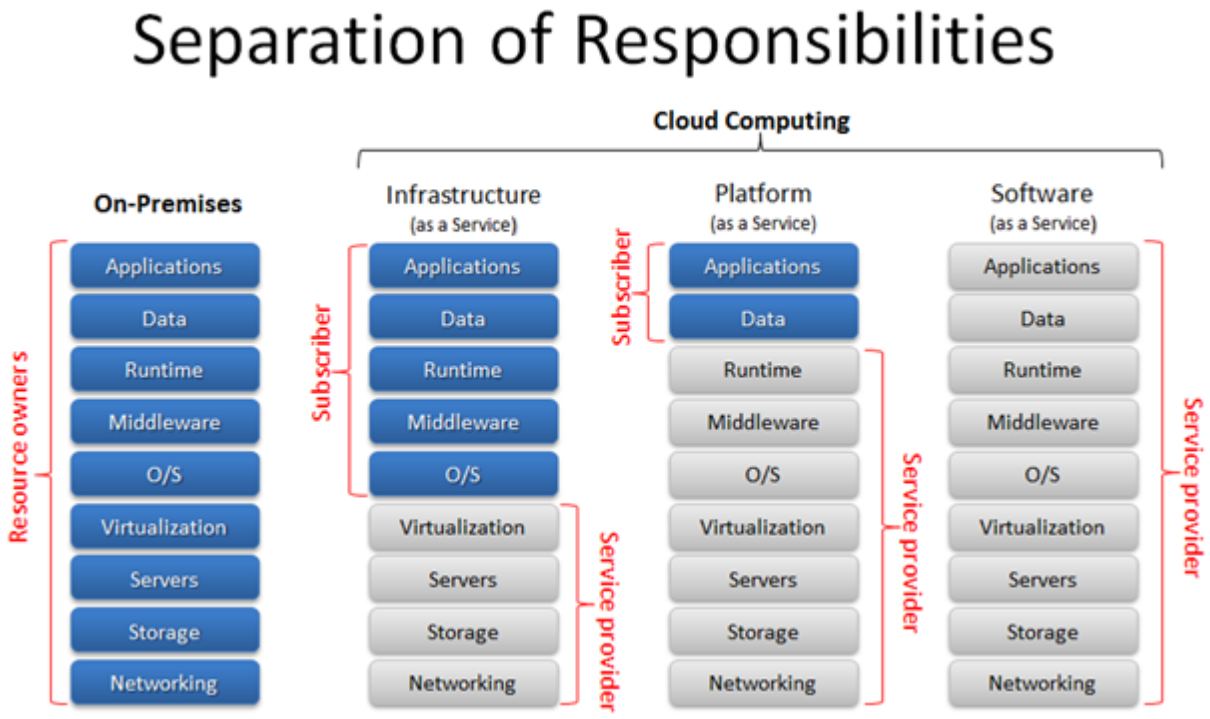

Figura nº 2. Modelos de servicio de la computación en la nube

3.2.4.-Otros modelos de servicio

Dentro de la anterior segmentación de servicios de computación en la nube (infraestructura, plataforma y software como servicios), se han planteado por los proveedores distinciones más específicas, como por ejemplo la seguridad como servicio, (SecaaS), la privacidad como servicio (PraaS), la base de datos como servicio (DBaaS) y un largo etcétera que ha originado la llamada "generación «*as a Service*»"[97]. Todos estos servicios deben entenderse integrados como subcategorías de los tres servicios anteriores (infraestructura, plataforma y software como servicios), ya que se prestan igualmente en entornos de computación en nube, y comparten las características descritas por el NIST[98].

4.- MODELOS DE IMPLEMENTACIÓN DE LA NUBE

Las compañías no suelen utilizar un sistema de computación en nube de

97 ALAMILLO DOMINGO, Ignacio. "El control de localización de los datos e informaciones en el Cloud", *Derecho y Cloud Computing*. (Coord. Ricard Martínez), 1ª Edición, Navarra, 2012, pág. 66.

98 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 6.

forma aislada, sino que, por lo general, combinan servicios *cloud* con sus propios equipos informáticos, en atención a sus especiales necesidades empresariales y teniendo en cuenta la complejidad de las cargas de trabajo que manejan y en qué medida se busca optimizar esas cargas. Los modelos de despliegue o implementación que explicaremos a continuación se han descrito por el NIST[99], y entre las ofertas existentes en el mercado, cada empresario cliente buscará aquella que mejor encaje con su operativa, su necesidad de control y el grado de compartición de los recursoss[100].

4.1.- Nube privada

En la definición del NIST, la nube privada es aquella en que "la infraestructura de la nube se suministra en exclusiva para una única empresa que integra múltiples usuarios (por ejemplo departamentos empresariales). Puede ser gestionada y operada por la propia organización, por un tercero, o en colaboración entre ambos, e instalarse dentro de las dependencias de la empresa (*on premises*) o en otro lugar (*off premises*)"[101].

La nube privada, también conocida como nube interna, opera en beneficio de un único gran cliente o de un conjunto de filiales pertenecientes al mismo grupo empresarial. Se crea con los recursos propios de la empresa, generalmente con la ayuda de proveedores especializados[102].

Cuando la nube privada se crea aprovechando el centro de datos del cliente como capa hardware (*on premise*), los procedimientos están más estandarizados, es decir, las operaciones se sujetan a ciertas instrucciones que detallan y explican el

99 NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …,op. cit.,* pág. 6.

100 ISO/IEC *International Standard 1788:2014 Information technology - Cloud computing - Overview and vocabulary* [en línea], 2014. Disponible en: <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>. [Fecha de consulta: 30 de marzo de 2017].

101 Así define el NIST la nube privada: "*the cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises"* (traducción propia). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …", op. cit.,* pág. 7.

102 Como servicios de nube privada, podemos citar: *Amazon Virtual Play Cloud* (ofrece una red virtual privada 100% controlable por el usuario), *Eucalyptus Cloud Platform* (ofrece un software de código abierto implementable en infraestructuras hardware del cliente y crear así una nube privada), *IBM Smart Cloud Foundation* (conjunto de soluciones que automatizan las operaciones del centro de datos del cliente) o *Microsoft Private Cloud* (ofrece virtualización y sistema operativo implementables en los recursos propios del cliente para dotar a estos de elasticidad y escalabilidad).

procedimiento para controlar la totalidad de la infraestructura y asegurar aspectos como el rendimiento técnico, la fiabilidad y la determinación de responsabilidades[103]. Así se consigue un sistema con las máximas garantías de seguridad y confidencialidad, pudiendo configurar todos sus detalles, aunque al estar limitadas a los centros de datos de la propia empresa cliente, la escalabilidad puede llegar a verse comprometida. Del mismo modo, generalmente la implementación de la nube privada sobre el hardware de la propia empresa implicará una inversión inicial de capital más o menos elevada con el fin de adaptar los equipos al nuevo entorno, se compensará mediante otras ventajas, tales como la máxima seguridad y protección de la información migrada[104].

Por contra, las nubes privadas hospedadas en centros de datos externos a la empresa permiten un máximo nivel de escalabilidad, porque el proveedor está habilitado para dedicar los recursos físicos al cliente cuando sus cargas de trabajo así lo requieran y garantizarle el máximo rendimiento en cuanto a procesamiento y almacenaje. Con estos recursos físicos exclusivos y no compartidos con otros clientes (es decir, sin "multi-tenencia"), se garantiza la total privacidad y una mayor protección contra accesos no autorizados, y se ahorra a través del pago por recursos consumidos y la no necesidad de actualización o mantenimiento de instalaciones físicas.

Independientemente de si la capa hardware pertenece al proveedor o la empresa cliente, con la nube privada se obtienen centros de datos virtualizados, interconectados y automatizados, con recursos físicos dedicados y procesos informáticos están sujetos a estrictos controles y monitorizaciones. Únicamente se implementan en las nubes privadas servicios de infraestructura y plataforma, puesto que las aplicaciones se ejecutarán dentro de las máquinas virtuales suministradas, para proteger al máximo la información gestionada a través de estas aplicaciones.

Por otra parte, la nube privada facilita la unidad de políticas internas en cuanto al manejo del centro de datos y el tratamiento de la información, permite la máxima personalización y favorece el trabajo corporativo entre sedes dispersas

103 ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf*, op. cit.*, pág. 10.

104 El modelo de nube privada es el que ofrece mayores garantías de seguridad, así que es el modelo ideal para el manejo de ciertos datos considerados críticos (*critical data*) que requieren extraordinaria protección. En estas nubes se instalan herramientas de seguridad de alto nivel, como cortafuegos especiales que salvaguarden el sistema de accesos no autorizados, *hackeado, malware* y demás acciones maliciosas.

geográficamente[105].

Este sistema de nube puede ser el más adecuado para grandes entidades cuyos datos requieren de un alto grado de confidencialidad y seguridad, y que son capaces de soportar el elevado coste inicial en inversión y mantenimiento. Lo adoptan administraciones públicas, hospitales, centrales nucleares, empresas de telecomunicaciones, corporaciones armamentísticas, entidades bancarias, etc.[106] Generalmente la inversión necesaria para implementar una nube privada no suele compensar las ventajas que pueda aportar a la generalidad de las pequeñas empresas. Aun así, existen proveedores que ofrecen este modelo a empresas pequeñas y medianas con especiales necesidades informáticas que dispongan de excelentes equipos propios o que busquen el máximo control sobre su infraestructura.

La contratación de una nube privada con un proveedor externo implica explícitos acuerdos contractuales y de nivel de servicio (*Service Level Agreement* o ANS) que probablemente se sometan a negociación. Como hemos comentado, dada la fuerte inversión inicial y el mantenimiento continuado que implica este modelo, el proveedor suele acceder a negociar un contrato individual con la empresa, donde se detallarán aspectos clave como las medidas de seguridad a adoptar y los principales protocolos de gobierno de la nube. Aun así, algunas de las cuestiones contractuales tratadas en este trabajo, el cual se centrará en la nube púbica, pueden ser de aplicación a contratos de nube privada.

4.2.- Nube comunitaria

Esta es la definición del NIST del modelo de nube comunitaria: "la infraestructura de la nube se suministra en exclusiva a una específica comunidad particular de usuarios, pertenecientes a organizaciones que comparten preocupaciones por temas específicos (por ejemplo, requieren medidas especiales de seguridad, o deben someterse a ciertas obligaciones legales específicas). Puede ser gestionada y operada por la propia comunidad, por un tercero, o en colaboración, e instalarse dentro de las dependencias de una o varias de las organizaciones (*on premises*) o en otro lugar (*off premises)*"[107].

105 ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf, *op. cit.*, pág. 10.

106 A modo de ejemplo, la Administración del Estado de Alaska implementó con este modelo sus infraestructuras de computación en la nube. Más información disponible en: <http://www.cisco.com/c/dam/en/us/solutions/collateral/data-center-virtualization/state_of_alaska_cs.pdf>. [Fecha de consulta: 30 de mayo de 2017].

107 Así define el NIST la nube comunitaria: "*The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on*

Así, nos encontraremos ante una nube comunitaria cuando dos o más organizaciones se alían para implementar una infraestructura *cloud* orientada a objetivos similares y dentro del mismo marco de seguridad y privacidad. Al compartir la infraestructura y recursos, se reducen los costes y el retorno de la inversión es más rápido que con la implementación de una nube privada individual para cada entidad miembro de la comunidad[108].

Algunos ejemplos de organizaciones que encajan en este modelo de despliegue son industrias farmacéuticas, administraciones públicas o entidades aseguradoras y financieras[109]. Como vemos, al igual que sucede con el modelo de nube privada, las pequeñas empresas no parecen tener en la nube comunitaria la mejor de sus opciones en cuanto a coste-eficiencia. Sin embargo, nada obsta a que se creen opciones por parte de los proveedores que aglutinen a pequeñas empresas con intereses similares y les ofrezcan compartir una nube comunitaria.

El suministro de los servicios *cloud* dentro de la nube comunitaria no difiere considerablemente de su prestación dentro de una nube privada, ni tampoco sus términos contractuales, que en su mayoría, al tratarse de grandes inversiones, suelen negociarse y configurarse *ad hoc* para aquella comunidad en especial.

4.3.- Nube pública

La nube pública, según el NIST, es aquella en que "la infraestructura *cloud* se suministra en línea para el público en general. Puede ser propiedad de una organización empresarial, organización académica o entidad pública, o varias de ellas, sobre quienes recaerá la administración y control. Se sustenta gracias a las instalaciones de un proveedor *cloud*"[110].

---

or off premises" (traducción propia). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 7.

108 INTECO, *Riesgos y Amenazas en Cloud Computing* [en línea], 2011. Disponible en <http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf>. [Fecha de consulta: 27 de junio de 2016]

109 A modo de ejemplo, algunos departamentos gubernamentales americanos comparten una nube comunitaria suministrada por Microsoft. La multinacional de servicios financieros NYSE Euronext acaba de extender a Europa su nube comunitaria: la *Capitol Markets Community Platform,* creada en 2011 con la colaboración de los proveedores líderes VMWare y EMC, juntamente con la división tecnológica de la propia NYSE: *NYSE Technologies*. Desde 2012, la asociación alemana de aseguradoras Gesamtverbandes der Deutschen Versicherungswirtschaft (o GDV) comparte el proyecto de nube comunitaria *Trusted German Insurance Cloud.*

110 En palabras del NIST, la nube pública es aquella en la cual: *"The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud*

En otras palabras, este modelo de implementación se ofrece a cualquier tipo de cliente, puesto que el acceso a este tipo de infraestructuras es mucho más económico y menos restrictivo. Aunque los recursos físicos están controlados siempre por un proveedor *cloud*, la nube pública puede ser titularidad de empresas privadas, gobiernos, etc[111].

Este modelo de nube presenta beneficios clave para particulares, empresas y organizaciones de todos los tamaños y sectores, puesto que es el modelo que ofrece una instalación más sencilla y una más rápida adaptación a la operativa empresarial del suscriptor, o que ha llevado a convertirla en el modelo más extendido y popular. El proveedor se responsabiliza por la instalación, aprovisionamiento, mantenimiento y gestión de los recursos físicos y lógicos, mientras el cliente queda liberado de adquirir y mantener hardware, aplicaciones y ancho de banda, porque el proveedor los suministra a través de Internet de forma escalable, y dedicarse únicamente a disfrutar de esos recursos. El uso de estos servicios de nube pública (infraestructura, plataforma y software como servicio), como veremos, se remunerarán de diferente manera, ya sea por recursos consumidos, facturándose mensualmente a modo de suministro, a modo de tarifa plana o mediante contraprestaciones no dinerarias, como la cesión de datos o la recepción de anuncios publicitarios de terceros[112].

Las nubes públicas ofrecen al cliente un entorno completo, flexible y elástico para que puedan procesar, compartir y almacenar datos según sus preferencias. Son sistemas pre-configurados pensados para que el cliente pueda instalarlos y operarlos sin necesidad de ayuda técnica por parte del proveedor, a modo de autoservicio automatizado, otorgándoles mayor rapidez, agilidad e independencia en la gestión de operaciones relacionadas con el uso del servicio. De esta manera, el pequeño empresario puede ser productivo incluso fuera de su oficina, a la vez que se facilitan los trabajos sincronizados entre usuarios de diferentes latitudes.

A la hora de delimitar el objeto de nuestra tesis doctoral, hemos decidido centrar nuestra atención en el modelo de implementación de nube pública, al ser el

---

provider" (traducción propia). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition …, op. cit.,* pág. 7.

111 Para facilitar la comprensión de este trabajo, nos referiremos a "proveedor de servicios en la nube" o "proveedor *cloud*" para aludir al titular de la nube que pone los recursos a disposición del suscriptor de los servicios. Sin embargo, debe tenerse en cuenta que entre el prestador final del servicio *cloud* y el proveedor de la capa de software pueden existir subcontrataciones.

112 Ver apartado "Obligaciones del suscriptor", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

más accesible y mayoritariamente suscrito por el pequeño empresario, sin perjuicio de que algunos aspectos del estudio puedan resultar de aplicación a otros entornos de nube. A pesar de todas sus ventajas, especialmente atractivas para el pequeño empresario y el consumidor, es el modelo que mayores problemas jurídicos presenta, al ser contratado masivamente a través de contratos de adhesión predispuestos por el proveedor, que el cliente debe suscribir en línea, sin posibilidad de someterlo a cambios o negociación alguna. Además de cuestiones sobre la calidad del servicio, la distribución de responsabilidades legales entre proveedor, cliente y subcontratistas y el contenido del deber de diligencia del proveedor y de la obligación del cliente de realizar un uso responsable del servicio, el contrato puede presentar, como veremos, cláusulas de dudosa adecuación a la legalidad y a la buena fe. Igualmente, pueden surgir dudas sobre la titularidad y la explotación de información alojada dentro de la nube, o problemas a la hora de recuperar los datos migrados una vez el servicio se dé por concluido.

El cumplimiento de la normativa sobre protección de datos es otro de los aspectos que pequeño empresario deberá tener en cuenta a la hora de contratar servicios de nube pública. Preocupan la deslocalización y los movimientos transfronterizos de datos de carácter personal (y en consecuencia, de falta de privacidad y potencial incumplimiento normativo), incluyendo la poca transparencia sobre el funcionamiento interno y la existencia de subcontrataciones de las cuales dependa la prestación, el control de la infraestructura subyacente, el compartimiento de recursos y las medidas de seguridad adoptadas[113].

Como se ha mencionado, todos estos aspectos serán objeto de un análisis jurídico que tendrá lugar en capítulos posteriores de este trabajo.

4.4.- Nube híbrida

Dice el NIST de la nube híbrida: "la infraestructura *cloud* es una combinación de dos o más modelos de implementación (privada, pública o comunitaria), que permanecen como entidades únicas (porque conservan las características de cada uno de los modelos implementados), pero su tecnología les permite compartir datos o aplicaciones entre ellas. Por ejemplo, el paso de una nube privada a una pública para sobrellevar picos de cargas de trabajo"[114].

113 INTECO, *Riesgos y Amenazas en Cloud Computing* [en línea], 2011. Disponible en <http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf>. [Fecha de consulta: 30 de marzo de 2017].

114 Original en inglés del NIST: *"The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by*

Se trata de un modelo en el que parte del servicio funciona a través de una nube privada o comunitaria, mientas que la parte restante opera a través de la nube pública. Pensemos en una empresa que desarrolla y prueba su aplicación en la nube privada, por razones de confidencialidad y seguridad, pero que la despliega en una nube pública para aprovechar su escalabilidad[115].

Como podemos deducir, la clave del buen funcionamiento de la nube híbrida se halla en un cuidadoso diseño a la hora de fraccionar los componentes que integran los modelos público y privado (o comunitario). Es el denominado *cloud bursting*, es decir, el paso de un modelo de nube a otro para aprovechar las ventajas de cada uno atendiendo a la demanda de recursos computacionales de cada momento[116].

La nube híbrida ofrece más flexibilidad que los modelos anteriormente explicados. En comparación con el modelo público, provee un control y seguridad más estrictos de los datos y aplicaciones. Por otra parte, permite las expansiones de servicio y la contratación bajo demanda que el modelo privado limita[117]. Este modelo en sí mismo aporta un óptimo aprovechamiento tanto de los recursos propios como de los proporcionados por el modelo público, usando y pagando por estos últimos solo cuando se necesitan (por ejemplo, en picos de cargas de trabajo), y sin tener que añadirlos al centro de datos propio de forma permanente. Por su parte, el segmento de la nube privado tiene las características, ventajas e inconvenientes mencionados antes e intrínsecos a todos los modelos privados de despliegue, al igual que sucede con el segmento público[118].

En resumen, la nube híbrida será la mejor elección para empresas que necesiten la máxima escalabilidad, pero que tengan especial preocupación por la seguridad. Así se pueden realizar aplicaciones no críticas (como interactuar con los

---

standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)" (traducción propia). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 800-145. The NIST Definition…, op. cit.*, pág.7.

115 A modo de ejemplo de nubes híbridas: *Microsoft Azure Stack*, o *HP Helion Cloud.* Como ejemplos de nubes híbridas especialmente dirigidos a pequeñas empresas, *VM Cloud Air Hybrid Service*, del proveedor VMWare, o *AppUpp,* de Intel.

116 Definición extractada de la página web oficial de la compañía tecnológica *Techtarget*, [en línea]. Disponible en <http://searchcloudcomputing.techtarget.com/definition/cloud-bursting>. [Fecha de consulta: 27 de junio de 2016]

117 ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf*, op. cit.,* pág. 10.

118 INTECO, *Riesgos y Amenazas en Cloud Computing* [en línea], 2011. Disponible en <http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf>. [Fecha de consulta: 3 de abril de 2017]

clientes o probar y ejecutar aplicaciones) en el segmento de nube pública, y aplicaciones críticas (tratar datos personales o confidenciales, o desarrollar nuevo software) dentro del segmento privado y con mejor seguridad. No obstante, debemos tener en cuenta que la administración de este tipo de modelo es compleja, porque al aunar entornos público, privado y centro de datos propio, la propia empresa cliente es responsable de su propio centro de datos y de la distribución de las cargas entre los segmentos privado y público de la nube[119].

5.-DEFINICIONES JURÍDICAS DE LA COMPUTACIÓN EN LA NUBE

En España, la normativa no recoge actualmente ninguna definición específica de la tecnología de computación en la nube, si bien a nivel europeo han existido algunas aproximaciones al concepto, como veremos. Tampoco en la jurisprudencia española se recoge, a día de hoy, ningún pronunciamiento sobre el contenido de esta nueva tecnología.

La Agencia Española de Protección de Datos publicó en su *Guía para clientes que contraten servicios de Cloud Computing* una aproximación al contenido de la computación en la nube. No reviste el formato de definición técnica, sino que se presenta de forma práctica y aclaratoria para el usuario: "El *Cloud Computing* o computación en nube es una nueva forma de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como para un particular y, también, para la Administración Pública. Una solución *Cloud Computing* permite al usuario optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información. El usuario no tiene necesidad de realizar inversiones en infraestructura, sino que utiliza la que pone a su disposición el prestador del servicio, garantizando que no se generan situaciones de falta o exceso de recursos, así como el sobrecoste asociado a dichas situaciones. En un entorno de *Cloud Computing*, la gestión de la información está de forma virtual en manos del cliente que contrata los servicios de la nube, que la trata a través de Internet accediendo a soluciones de bases de datos, correo electrónico, nóminas o gestión de recursos humanos de acuerdo a sus necesidades"[120].

Aunque esta aclaración no posee categoría normativa ni carácter vinculante

119 KALPANA, P; LAHARIKA, M. "A comparative Study of Different Deployment Models in a Cloud", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, 2013, pág. 514.

120 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía para clientes que contraten servicios de Cloud Computing 2013* [en línea]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf>. [Fecha de consulta: 3 de abril de 2017]. Ver apartado "La importancia del contrato entre proveedor y cliente. Las políticas de privacidad", en el capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

alguno, sí puede tenerse en cuenta a efectos de distinción de tecnologías preexistentes, como la distribución física de paquetes de software (por ejemplo, un conjunto de discos con programas ofimáticos) o la gestión de información mediante un centro de datos propio con hardware y capacidades informáticas limitadas. No obstante, es precisamente su naturaleza de mera "guía" o "recomendación" lo que impide que pueda tener trascendencia jurídica más allá de aportar un criterio interpretativo relevante.

En el ámbito de la Unión Europea, la Comisión Europea, consciente del potencial de la computación en la nube, adoptó en el año 2012 una estrategia para promover su rápida adopción en todos los sectores de la economía con el fin de impulsar la productividad. Esta estrategia se adoptó mediante la Comunicación titulada *Unleashing the Potential of Cloud Computing in Europe* COM(2012) 529 final, de fecha 27 de septiembre de 2012. Tiene tres objetivos fundamentales: conseguir unas condiciones contractuales "seguras y justas"; establecer estándares que permitan la interoperabilidad, portabilidad de datos y reversibilidad; y desarrollar el *European Cloud Partnership*, un organismo de colaboración en materia de *Cloud Computing* que integre a la industria y al sector público[121].

Asimismo, se creó por la propia Comisión el Grupo de Expertos en contratos de *Cloud Computing*, compuesto por profesionales y representantes del sector, por organizaciones defensoras de consumidores y de pequeñas empresas y por expertos y académicos en materia legal. Sus tareas se centraban en el asesoramiento en materia contractual y desarrollar unas condiciones contractuales modelo que fueran equitativas para consumidores y pequeñas empresas que contrataran servicios de computación en la nube, y que recogieran aspectos como la conservación de los datos una vez finalizada la relación contractual, la seguridad y revelación de datos, la ubicación y transferencia de datos, la propiedad de datos y la distribución de responsabilidades entre cliente, proveedor y subproveedores[122].

---

121 Todo ello para conseguir, en 2020 y según las previsiones, 2,5 millones de puestos de trabajo en Europa y unos beneficios de 160 billones de euros, lo que implicaría un aumento del producto interior bruto de un 1%. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>. Sitio web oficial de la *European Cloud Computing Strategy* de la Comisión Europea disponible en: <https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy>. [Fecha de consulta: 3 de abril de 2017].

122 El Grupo de Expertos en contratos de *Cloud Computing* se creó mediante la Decisión de 18 de junio de 2013 2013/C 174/04. Disponible en: <http://eur-

En la mencionada Comunicación *Unleashing the Potential of Cloud Computing in Europe* se describe así a la computación en nube: "La computación en nube, en términos generales, puede entenderse como el almacenamiento, procesamiento y utilización de datos en sistemas informáticos ubicados remotamente y a los cuales se accede a través de Internet. Significa que los usuarios pueden disponer de recursos informáticos prácticamente ilimitados bajo demanda, sin necesidad de realizar inversiones en infraestructura para satisfacer sus necesidades, y pudiendo acceder a sus datos desde cualquier dispositivo con conexión a Internet. El *Cloud Computing* tiene la capacidad de recortar los dispendios en IT del usuario y pone a su disposición multitud de servicios. Con el uso de la nube, incluso las más pequeñas empresas pueden expandirse hacia grandes mercados y las Administraciones pueden ofrecer sus servicios de un modo más atractivo y económico"[123].

Además de la Comisión Europea, según el Grupo de Trabajo del Artículo 29 (creado por la Directiva de Protección de Datos 95/46/CE)[124] "El *Cloud Computing* consiste en un conjunto de tecnologías o modelos de servicio que se centran en el suministro a través de Internet de aplicaciones de Tecnologías de la Información, capacidad de procesamiento, espacio de memoria y almacenaje. La nube puede generar grandes beneficios económicos porque los recursos pueden ampliarse, configurarse y accederse fácilmente a través de Internet, siempre ajustados a las necesidades de la demanda. Además, ayuda a incrementar la seguridad, puesto que las pequeñas y empresas, por un coste marginal, pueden adquirir tecnologías de alto nivel que de otro modo sobrepasarían las previsiones presupuestadas para inversión tecnológica"[125].

---

lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2013:174:0006:0008:EN:PDF>. Los informes elaborados por el Grupo de Expertos están disponibles en el sitio web oficial de la Comisión Europea. <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 3 de abril de 2017]. Algunas de estas materias, si bien han sido objeto de discusión e informes preparatorios por parte del Grupo de Expertos, no se han visto reflejadas todavía en un código de conducta que proteja a pequeños empresarios y consumidores de servicios *cloud* de eventuales prácticas abusivas por parte de proveedores. Más información sobre la European Cloud Computing Strategy disponible en: <https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy>. [Fecha de consulta: 3 de abril de 2017].

123 Traducción propia del original en inglés: "*Cloud Computing' in simplified terms can be understood as the storing, processing and use of data on remotely located computers accessed over the Internet. This means that users can command almost unlimited computing power on demand, that they do not have to make major capital investments to fulfil their needs and that they can get to their data from anywhere with an Internet connection. Cloud computing has the potential to slash users' IT expenditure and to enable many new services to be developed. Using the cloud, even the smallest firms can reach out to ever larger markets while governments can make their services more attractive and efficient even while reining in spending".*

124 En su Dictamen 05/2012 sobre la computación en la nube (WP 196) [en línea], el Grupo de Trabajo del Artículo 29 recoge los principales riesgos que supone el *Cloud Computing* para la protección de los datos personales, y los roles de cada uno de los actores que intervienen en el tratamiento, así como las cuestiones relacionadas con la transferencia internacional de datos. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en .pdf>. [Fecha de consulta: 3 de abril de 2017]. Ver capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

125 *Traducción propia del original en inglés: "Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. Cloud computing can generate important economic benefits, because on-demand resources can be configured, expanded and accessed on the Internet quite easily. Next to economic benefits,*

Esta definición, al igual que la anterior, presenta la computación en la nube como un eventual beneficio para empresas y Administraciones, y el plan estratégico europeo pretende impulsar la rápida adopción de sistemas de computación remota en los sectores público y privado, para estimular la productividad[126]. A nuestro modo de ver, aunque aún no se haya plasmado materialmente en la normativa comunitaria, los actuales trabajos en materia de protección de datos pueden ser el inicio de una serie de regulaciones relacionadas con otros aspectos legales de la computación en nube, como podrían ser la competencia, la propiedad intelectual o la protección al consumidor y al pequeño empresario[127].

A nuestro parecer, esta definición cumple con el objetivo de delimitar las técnicas informáticas que puedan considerarse como "computación en la nube" a los simples efectos de aplicar normas de protección de datos personales cuando el responsable haga uso de este tipo de infraestructuras para su tratamiento, valiéndose para ello de centros de datos externalizados en los que los datos puedan verse comprometidos. Por esta razón, la norma limita el uso de la nube para tratar datos personales al cumplimiento de ciertos requisitos que garanticen la debida protección de tales datos.

Aunque esta definición probablemente se quede corta si lo que se pretende es abarcar problemática jurídica diferente a la protección de datos personales (lo que en este caso lógicamente no sucede puesto que el ámbito objetivo del Reglamento mexicano es la protección de datos personales en posesión de particulares), valoramos positivamente que el propio artículo 52 exija transparencia en las subcontrataciones, obligue al proveedor a comunicar eventuales cambios no solo en las políticas de privacidad sino también en la condiciones de prestación del servicio,

---

cloud computing may also bring security benefits; enterprises, especially small-to-medium sized ones, may acquire, at a marginal cost, top-class technologies, which would otherwise be out of their budget range".

126 Para ello se creó la iniciativa *Cloud for Europe* (C4E), dentro de la *European Cloud Partnership*, para identificar obstáculos y generar confianza en la tecnología *Cloud* mediante la colaboración entre el sector público y la industria del sector *Cloud*. información disponible en: <http://www.cloudforeurope.eu>. [Fecha de consulta: 3 de abril de 2017].

127 Como hemos mencionado, el Grupo de trabajo del Artículo 29 de la Comisión Europea adoptó, en julio de 2012, el Dictamen 05/2012 sobre computación en la nube, que trata las principales cuestiones sobre protección de datos que afectan a proveedores y usuarios de *Cloud Computing* residentes en la Unión Europea, y sobre cómo se les aplican las Directivas 95/46/CE sobre protección de datos y 2002/58/CE (modificada por la 2009/136/CE) sobre protección de datos en el sector de las telecomunicaciones. Disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm>. [Fecha de consulta: 3 de abril de 2017].

y que deba procederse al borrado de datos personales que puedan permanecer en la infraestructura una vez extinguida la relación entre proveedor de la nube y responsable del tratamiento.

6.- ALGUNAS CONSIDERACIONES SOBRE LA COMPUTACIÓN EN LA NUBE. EN PARTICULAR, PRINCIPALES VENTAJAS Y RIESGOS

Son muchos los beneficios que ofrece la nube no solo para el sector empresarial, sino también para los particulares y los organismos públicos[128]. En resumen, sus mayores ventajas son: el ahorro de costes en inversión, mantenimiento, actualizaciones y mejoras de la infraestructura informática; la disminución de los costes del aprovisionamiento excesivo; la arquitectura en capas del sistema (que permite acceder de manera flexible a las capacidades que el cliente realmente demanda) y su fiabilidad; la accesibilidad inmediata y desde cualquier dispositivo sin necesidad de elevados conocimientos técnicos (sobre todo para el software como servicio o SaaS); y la facilidad para compartir y actualizar contenidos, aplicaciones y demás recursos computacionales tanto dentro de la propia organización como con terceros.

Gracias a estos incentivos, la nube actualmente se presenta como revolucionaria, mueve un elevado capital económico y de información, y manifiesta una clara tendencia a convertirse en un servicio de consumo generalizado y con gran impacto dentro de la sociedad tecnológica que nos rodea. Por estas y otras razones, el impacto económico de la computación en la nube se ha estimado en 940 billones de euros y en 3,8 millones de puestos de trabajo para el período 2015-2020[129].

Desde el punto de vista empresarial, existe una gran competencia por obtener

128 GARCÍA SÁNCHEZ, Manuel, "Retos de la computación en la nube", *Derecho y Cloud Computing.* (Coord. Ricard Martínez), 1ª edición, Navarra, 2012, págs. 39 a 40, 45.

129 IDC, *Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake* [en línea], 2012. [Fecha de consulta: 27 de junio de 2016] Disponible en: <http://ec.europa.eu/digital-agenda/en/news/quantitative-estimates-demand-cloud-computing-europe-and-likely-barriers-take-final-report>. Se ha llevado a cabo un seguimiento del anterior informe, cuyos resultados se publican en otro informe final para la Comisión Europea: IDC, *SMART 2013/0043 - Uptake of Cloud in Europe. Follow-up of IDC Study on Quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up* [en línea], 2015. Disponible en: <https://ec.europa.eu/digital-agenda/en/news/final-report-study-smart-20130043-uptake-cloud-europe>. [Fecha de consulta: 27 de junio de 2016].

una posición de poder en el mercado, tanto de las empresas del sector TIC como de otras industrias, y la adaptación a las tecnologías emergentes se manifiesta como un aspecto clave para el éxito empresarial. La sociedad desea la conectividad, el acceso a las más inteligentes herramientas tecnológicas y la máxima accesibilidad a datos.

Para finalizar con este capítulo, y con el objetivo de completar la aproximación a la realidad de la contratación de servicios de computación en la nube, analizaremos la situación actual relativa a la adopción de entornos en la nube por el pequeño empresario español y cuáles son las razones que impiden una mayor implementación en el tejido empresarial, entre las que se encuentran algunas cuestiones referentes a su regulación jurídica.

6.1.-Implementación de la computación en la nube por el sector empresarial en la actualidad. Ventajas

Las empresas han encontrado en la nube una forma de abastecerse de capacidad de procesamiento, almacenaje y aplicaciones sin tener que adquirir una mayor o más potente infraestructura informática, y sin tener que actualizar constantemente su software, lo cual disminuye considerablemente el coste económico, en recursos humanos y en tiempo de adaptación a la nueva tecnología. Este acceso se producirá de forma inmediata, ininterrumpida y automática, a través de una plataforma web que permitirá manejar estas capacidades, de acuerdo con las necesidades y cargas de trabajo que precise el empresario en cada momento, y a medida que desarrolla su actividad económica principal[130].

A continuación, efectuaremos unos breves apuntes sobre la situación actual de la implementación de servicios de *Cloud Computing* en las PYMEs españolas.

130 Por otra parte, su implementación posibilita un mejor manejo del *Big Data,* una tecnología que permite capturar, almacenar, compartir y analizar grandes cantidades de datos que superan la capacidad convencional de procesamiento de las herramientas informáticas tradicionales, y que tiene aplicaciones, por ejemplo, en el *marketing* digital o en la elaboración de estadísticas, estudios o previsiones de comportamientos de los consumidores que ayudan significativamente en la toma de decisiones empresariales. El *Big Data* ha sido definido como "extensos conjuntos de datos, atendiendo principalmente a las cualidades de volumen, variedad, velocidad, y/o disponibilidad, que requieren de una arquitectura escalable para un almacenamiento, manejo y análisis eficiente". NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST, *Special Publication 1500-1. Big Data Interoperability Framework: Volume 1: Definitions* [en línea], 2015, pág. 4. Disponible en: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1.pdf>. [Fecha de consulta: 27 de junio de 2016]. Sobra decir que todas estas utilidades del Big Data son igualmente valiosas para el sector turístico.

Según los datos del Instituto Nacional de Estadística, el tejido empresarial español, a fecha de 1 de enero de 2016, estaba formado por un 95,7% de microempresas (de 0 a 9 empleados) y por un 3,6 % de pequeñas empresas (de 10 a 49 empleados). Todo ello frente a un porcentaje de 0,6% de medianas empresas (de 50 a 199 empleados) y de un 0,1% de grandes empresas (más de 200 empleados)[131]. Estos datos evidencian la importancia de la microempresa y la pequeña empresa en la economía española. Conscientes de esta situación, hemos enfocado nuestro trabajo a microempresarios, pequeños y medianos empresarios que decidan contratar servicios de computación en la nube e incorporarlos en su actividad empresarial, ya que, por sus dimensiones, carecen de poder de negociación, viéndose obligados a suscribir las condiciones generales predispuestas por el proveedor y sin que, en principio, puedan beneficiarse de la protección ante comportamientos abusivos que ampara al consumidor[132].

Cabe mencionar que el grado de penetración de la tecnología de computación en la nube en estas empresas es todavía bajo, puesto que solo un 5,4% de las microempresas adquirieron en 2015 algún servicio *cloud,* cayendo 3 puntos en comparación con el año anterior[133]. Entre los servicios de computación en la nube más adquiridos en el primer trimestre de 2016 por las empresas españolas de más de 10 empleados, destacan el almacenamiento de ficheros (68,7%) y el correo electrónico (71,2%)[134]. Aunque siguen siendo menos comunes en la pequeñas

131 Según los datos del *Retrato de la PYME - DIRCE a 1 de enero de 2016*, publicado en febrero de 2017 y elaborado por el Instituto Nacional de Estadística (INE) y publicado en enero de 2016, a 1 de enero de 2016 existían en España 3.232.706 empresas, de las cuales el 99,8% son PYMEs (es decir, tienen entre 0 y 249 asalariados). Así, el conjunto de empresas formado por microempresas y pequeñas y medianas empresas (englobadas como PYMEs), representan el 99,9 % del tejido empresarial español, mientras que las grandes compañías (de 250 o más empleados) únicamente suponen el 0,1% del total de empresas españolas. INSTITUTO NACIONAL DE ESTADÍSTICA INE, *Retrato de la PYME- DIRCE a 1 de enero 2016* [en línea], 2016. Disponible en: <http://www.ipyme.org/publicaciones/retrato-pyme-dirce-1-enero-2016.pdf>. [Fecha de consulta: 23 de marzo de 2017].

132 A todos ellos nos referiremos en este trabajo como "pequeños empresarios".

133 Datos según los informes *Análisis sectorial de la implementación de las TIC en la PYME española,* elaborado por la Fundación para el Desarrollo Infotecnológico de Empresas y Sociedad (FUNDETEC) y el Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (ONTSI). FUNDETEC; ONTSI; Informes ePYME 2014 y e-PYME 2015. *Análisis sectorial de la implementación de las TIC en la PYME española,* [en línea], 2014 y 2015. Disponibles respectivamente en. <http://www.ontsi.red.es/ontsi/sites/default/files/informe_epyme14_analisis_sectorial_de_implantacion_de_las_tic_en_la_pyme_espanola_0.pdf> y <http://www.ontsi.red.es/ontsi/sites/ontsi/files/e-pyme_15_analisis_sectorial_de_implantacion_de_las_tic_en_la_pyme_espanola.pdf>. [Fecha de consulta: 29 de marzo de 2017]

134 Estos datos se desprenden de la *Encuesta sobre el Uso de las Tecnologías de la Información y*

empresas (12,8 %), la tendencia apunta a que la contratación de estos servicios crece a medida que aumenta el tamaño de la empresa[135]. Para mejorar la competitividad de la PYME española, las Administraciones Públicas impulsan el salto a la nube para las pequeñas empresas, a través de programas de ayudas e instrumentos de difusión de las ventajas del *Cloud Computing,* y desarrollo de nuevas plataformas basadas en esta tecnología[136].

Entre otras virtudes, el *Cloud Computing* permite a las empresas mejorar las experiencias de sus clientes y desarrollar la comunicación, colaboración y coordinación en tareas y proyectos con sus trabajadores y socios comerciales. Supone un profundo cambio en la manera de trabajar, y para ello será esencial la preparación de los directivos y empleados en temas de seguridad informática y confidencialidad de los datos que maneja la empresa. Estas ventajas motivan un crecimiento que se prevé exponencial en su adopción, mayor en los modelos de implementación pública y en el tráfico de datos, estimando que el modelo de servicio más extendido sea el software como servicio, seguido de los modelos de infraestructura y plataforma, y se pronostica que más de dos billones de usuarios de Internet (el 55% del total) utilizarán en 2019 servicios de almacenamiento en la nube[137].

---

las Comunicaciones (TIC) y del comercio electrónico en las empresas. Año 2015- 1er Trimestre 2016 [en línea], realizada por el Instituto Nacional de Estadística, y cuyos resultados se publicaron en junio de 2016. Disponible en: <http://www.ine.es/prensa/np978.pdf>. [Fecha de consulta: 29 de marzo de 2017].

135 Así lo afirma el informe del Observatorio Nacional de las Telecomunicaciones y los Sistemas de Información ONTSI titulado *La sociedad en Red. Informe Anual 2015. Edición 2016*, [en línea] publicado en septiembre de 2016, págs. 17, 23, 129. Disponible en: <http://www.ontsi.red.es/ontsi/es/content/informe-anual-la-sociedad-en-red-2015-edici%C3%B3n-2016>. [Fecha de consulta: 29 de marzo de 2017].

136 En mayo de 2016, el Ministerio de Energía, Turismo y Agenda Digital destinó más de 40 millones de euros en ayudas a PYME de cualquier sector, con menos de 250 empleados, para que adoptasen soluciones basadas en tecnología *Cloud Computing*, mediante la campaña "Súbete a la nube. Programa de Fomento de soluciones de *Cloud Computing* dirigido a PYMEs". Nota de prensa oficial del Ministerio disponible en: <http://www.red.es/redes/es/sala-prensa/notas-prensa/el-ministerio-de-industria-energia-y-turismo-destina-40-millones-de-eu>. En 2017, se destinan 18,3 millones de euros para que 360 PYME (en este caso, empresas proveedoras del sector TIC) generen nuevas soluciones de *Cloud Computing*. Nota de prensa oficial del Ministerio de Energía, Turismo y Agenda Digital disponible en: <http://www.red.es/redes/sala-de-prensa/noticia/mas-de-360-pymes-del-sector-tic-se-repartiran-183-millones-para-generar-nueva>. [Fecha de consulta: 29 de marzo de 2017].

137 El quinto informe anual CISCO *Cloud Global Index, Forecast and Methodology*, publicado en octubre de 2015, estima un crecimiento de la nube pública a un ritmo interanual del 44% entre 2014 y 2019, mientras que para la nube privada se augura un crecimiento del 16% interanual durante el mismo período. Predice que el tráfico *cloud* global se cuadruplicará, ya que se prevé que

En el ámbito turístico, el *Cloud Computing* también tiene notable influencia, como se verá más detalladamente en el capítulo expresamente dedicado a la computación en la nube en el sector turístico[138]. En el sector de alojamiento y agencias de viajes, muchas de las empresas utilizan redes sociales (un 73,8% de microempresas del sector) para intercambiar opiniones con sus clientes y como herramienta de difusión de la imagen empresarial y otras estrategias de *marketing*[139]. Otros servicios *cloud* que suscriben las microempresas del sector turístico son el correo electrónico, el almacenamiento de ficheros y el software como servicio destinado a tratar informaciones de clientes. Los principales motivos que frenan su adopción son el insuficiente conocimiento sobre la tecnología *cloud*, la apreciación por algunas empresas de su falta de necesidad de implementación de sistemas *cloud* en su operativa, el coste o la sensación de inseguridad jurídica.

Sin embargo, el *Cloud Computing* tiene mucho que ofrecer a un sector que depende, en buena medida, del conocimiento de los gustos del cliente y de una estrecha comunicación con este. Por ello resulta necesario, bajo nuestro punto de vista, dar a conocer al pequeño empresario la existencia de estas tecnologías y de sus

---

de los 2,1 *Zettabytes* anuales registrados en 2014, se alcancen un total de 10,4 *Zettabytes* anuales a finales de 2019, lo que supone un crecimiento de un 33% anual. Un *Zettabyte* corresponde a 10^{21} *bytes*, o a mil millones de *Terabytes*, y es la segunda unidad máxima de medida de la capacidad de almacenamiento de información digital inventada hasta el momento, sobrepasada únicamente por el *Yottabyte*. El mismo organismo CISCO, para aproximar una idea del volumen de datos que implican estas cifras, pone como ejemplo en su nota de prensa sobre este informe, que 10,4 *Zettabytes* equivalen a un tráfico anual de 114 trillones de horas de música en streaming o a 6.8 trillones de películas en alta definición (HD). En cuanto a los modelos de servicio, se prevé que, de la implementación de servicios *cloud* en entornos públicos y privados, un 59% corresponderá a software como servicio, y un 30% a infraestructura como servicio, y únicamente un 11·% corresponderá a plataforma como servicio. CISCO *Cloud Global Index, Forecast and Methodology* [en línea], 2015. Disponible en: <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.pdf> y <https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1724918>. [Fecha de consulta: 24 de junio de 2016].

138 Este trabajo se ha realizado en el marco del proyecto DER2015-63595-R "*Big Data, Cloud Computing* y otros nuevos retos jurídicos planteados por las tecnologías emergentes; en particular, su incidencia en el sector turístico" (Investigadora principal: Apol·lònia Martínez Nadal), financiado por el Ministerio de Economía y Competitividad y desarrollado en la Universitat de les Illes Balears. Además, este trabajo ha tenido lugar gracias a la ayuda de una beca otorgada por la *Conselleria d' Innovació, Recerca i Turisme* del *Govern de les Illes Balears* y del Fondo Social Europeo, en el marco del Programa Operativo FSE 2014-2020.

139 Aunque un 41,8% de empresas utilizan software empresarial de gestión de clientes (CRM) y un 28,7% utilizan aplicaciones de planificación de recursos (ERP), el informe no especifica si el software tomado como referencia para el estudio se consume a modo de programa informático tradicional o como software como servicio (SaaS), o si se tienen en cuenta ambas modalidades.

beneficios, concienciar de la idoneidad de la adopción de sistemas de computación en la nube como una medida impulsora de la competitividad y del crecimiento del negocio, y, especialmente, favorecer su adecuada protección jurídica frente a los proveedores de estos servicios cuando de su utilización puedan derivarse responsabilidades legales, en favor de una mayor confianza en estos sevicios.

Por otro lado, el sector turístico se encuentra sometido a un constante cambio debido a la evolución tecnológica: se perfila el nuevo turista 2.0, aparecen nuevos modelos de negocio turístico basado en esta tecnología (agencias de viaje en línea u OTAs, comparadores de ofertas, plataformas de opiniones, aplicaciones informáticas enfocadas a mejorar la operativa empresarial o a personalizar la experiencia del turista, inclusión en establecimientos hoteleros de la llamada *Internet of Things*, etc.) y múltiples empresas tradicionales se aprovechan de los beneficios de alojar información en servidores remotos, gestionar su actividad empresarial desde cualquier dispositivo u ofertar sus servicios con publicidad personalizada a través de las redes sociales. Por ello, la empresa turística que quiera aprovecharse de la innovación y adquirir tanto una mejor posición en el mercado como un mayor contacto con su clientela habitual y potencial, deberá considerar seriamente la posibilidad de suscribir servicios de computación en la nube[140].

6.2.- Riesgos de la implementación del *Cloud Computing* por parte de las empresas

La *migración* a la nube, que es como se denomina al traslado de la

140 El sector turístico se constituyó como fundamental en la economía de nuestra Comunidad Autónoma, las Islas Baleares. Según datos de diciembre de 2014, según el 45% del PIB de esta comunidad está vinculado a la actividad turística, y el sector turístico balear representa el 10% del total del impacto económico de España. Así se desprende del *Estudio de Impacto Económico del Turismo sobre la Economía y el Empleo de las Islas Baleares, IMPACTUR 2014* [en línea], elaborado por el *Govern de les Illes Balears* y la asociación sin ánimo de lucro para la excelencia turística Exceltur. Disponible en: <http://www.exceltur.org/impactur/>. [Fecha de consulta: 29 de marzo de 2017]. Por su parte, el *Govern de les Illes Balears* define al archipiélago balear como "un destino vanguardista, sede de empresas turísticas con proyección internacional", y en el cual reside una diversificada oferta de turismo con "una arraigada experiencia en gestión turística, un buena dotación de recursos, una amplia oferta complementaria y una cultura empresarial centrada en la calidad y la excelencia". Extractado del sitio web *Investinbalearics.com*, destinado a la promoción de Baleares como destino de inversiones nacionales y extranjeras, propiedad de la Consejería de Economía y Competitividad de las Islas Baleares. Disponible en: <http://www.investinbalearics.com/web/sectors/tourism.php>. [Fecha de consulta: 29 de marzo de 2017].

información del cliente a la infraestructura en red que suministra el proveedor, implica ciertos riesgos que cualquier empresa debe ponderar[141]. Aunque algunos de ellos son conocidos, la mayoría de pequeñas y medianas empresas no son plenamente conscientes de su potencial impacto económico y reputacional (ni tampoco los consumidores)[142]. A continuación, analizaremos los riesgos que implica la utilización

141 Para esta clasificación de riesgos, hemos tomado como referentes los trabajos al respecto elaborados por diferentes entidades: la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), la *European Network and Information Security Agency* (ENISA); el Instituto Nacional de Tecnologías de la Información INCIBE (antes INTECO), el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la información (ONTSI), la Cloud Security Alliance (CSA) y el capítulo de Kuan Hon y Christopher Millard . Todos ellos se citan a continuación. GRUPO DE TRABAJO IV, CNUDMI, *Aspectos contractuales de la computación en la nube A/CN.9/WG.IV/WP.142* [en línea], pág. 17, disponible en: <http://www.uncitral.org/uncitral/es/commission/working_groups/4Electronic_Commerce.html>. ENISA, *Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información* [en línea], 2009; y *Cloud Security Guide for SMEs. Cloud security Risks and Oportunities for SMEs* [en línea], 2015. Disponibles respectivamente en: <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish> y <https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes>. INCIBE (antes INTECO), *Riesgos y Amenazas en Cloud Computing* [en línea], 2011. Disponible en: <http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf>. INCIBE (antes INTECO), *Guía para empresas: seguridad y privacidad del Cloud Computing* [en línea], 2011. Disponible en: <http://www.inteco.es/CERT/guias_estudios/guias/Guia_Cloud>. ONTSI, *Cloud computing. Retos y oportunidades* [en línea], 2012. Disponible en: <http://www.ontsi.red.es/ontsi/es/estudios-informes/cloud-computing-retos-y-oportunidades>. *Cloud Security Alliance* CSA, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1* [en línea], 2009. Disponible en <https://cloudsecurityalliance.org/research/security-guidance/>. HON, W. Kuan; MILLARD, Christopher, "Control, Security and Risk in the Cloud", *Cloud Computing Law* (Coord. Christopher Millard), 1ª edición, Oxford, 2013, págs. 18 a 35. [Fecha de consulta: 30 de mayo de 2017].

142 Según el informe *Más allá de las buenas intenciones. La necesidad de pasar de las intenciones a la acción con el fin de controlar el riesgo de la información en las medianas empresas*, elaborado por la consultora *PwC* en colaboración con la empresa de gestión de activos de información *Iron Mountain* y presentado en julio de 2014, "apenas un 37% de las medianas empresas europeas y un 47% de las norteamericanas cuentan con una estrategia de riesgo de la información totalmente supervisada". Según afirma el estudio, "esta debería ser la base sobre la que apoyen las medidas de protección adecuadas, aunque más de la mitad de las medianas empresas no lo está haciendo". En palabras del responsable de riesgo de la información de *Iron Mountain*, Christian Toon, para este mismo informe, "desde la más grande y consolidada hasta la mediana de reciente creación, las empresas se ven incapaces de salvar las distancias entre contar con un plan o una política bienintencionados y asegurarse de que realmente funciona". IRON MOUNTAIN; PwC; *Más allá de las buenas intenciones. La necesidad de pasar de las intenciones a la acción con el fin de controlar el riesgo de la información en las medianas empresas* [en línea]. Disponible en: <http://www.ironmountain.es/riesgo-informacion/~/media/94CCAD64A20F408EB2BF44F2AFCA8710.p df>. [Fecha de consulta: 27 de junio de 2016]

de servicios de computación en la nube.

6.2.1.- Riesgos organizativos

Como puede deducirse a primera vista, una de las principales desventajas que presenta la computación en nube es la dependencia del proveedor o proveedores que prestan todo o parte del servicio. Existen múltiples vicisitudes que pueden tener lugar durante el transcurso de la relación profesional entre el cliente y el proveedor, y que pueden afectar a los datos que el cliente ha migrado a la nube, a la prestación y disponibilidad del servicio y al prestigio de la compañía suscriptora de los servicios. Por ejemplo, la discontinuidad de la prestación o la aparición de eventuales contratiempos relacionados con la seguridad de los sistemas.

Como consecuencia de estos problemas, el cliente *cloud* que decida terminar el contrato y cambiar de proveedor puede encontrarse con serias dificultades para recuperar sus datos[143], asegurarse de su borrado efectivo de los equipos del antiguo proveedor y gestionar la migración hacia la nueva nube[144]. La problemática de recuperación de la información migrada se agravaría en caso de que la empresa proveedora del servicio de computación en la nube se declarase en quiebra, fuera absorbida o adquirida por otra con diferentes políticas comerciales, o cerrada por las autoridades[145].

---

143 Si los contenidos comparten los estándares de la industria de la computación en la nube, o si tienen un formato libre (es decir, un formato abierto, sin restricciones de uso legales o económicas), es más fácil y rápido migrar los datos hacia otro entorno en caso de contingencia o terminación contractual, y que esos datos sean interoperables. En caso contrario, si el proveedor o un tercero son (o pretenden ser) los titulares del formato de los datos, aplicaciones o interfaces, puede ser caro o dificultoso exportarlos a un formato que permita su reutilización en otros entornos. Actualmente se están llevando a cabo tareas de promoción de estandarización por diferentes organizaciones, como la DMTF (*Distributed Management Task Force, Inc*), el *European Telecomunications Standard Institute* (ETSI), el *Global Inter-Cloud Technology Forum* (GICTF) o el *Open Grid Forum*. Todos ellos cuentan con miembros de las principales empresas del sector para crear desarrollar especificaciones y estándares de los elementos software que integran el entorno de la computación en nube. Más información en la página *Cloud Standards Wiki*. Disponible en: <http://cloud-standards.org/wiki/index.php?title=Main_Page>. [Fecha de consulta: 6 de julio de 2016].

144 Ver ROSSELLÓ RUBERT, Francisca Mª, "La recuperación de los contenidos alojados y su portabilidad; en especial, su previsión por el Reglamento 2016/679 General de Protección de Datos de la UE", *Hacia una justicia 2.0, Actas del XX Congreso Iberoamericano de Derecho e Informática* (Dir. Federico Bueno de Mata), Salamanca, 2016, págs. 283 a 298. Asimismo, ver capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

145 Recordemos el caso *Megaupload*, en el año 2012. Las autoridades americanas decretaron el cierre de esta nube de descarga y almacenaje por infracción de derechos de propiedad intelectual

Debe tenerse en cuenta que el grado de dependencia varía según el tipo de nube implementada y el servicio suscrito, así como las relaciones existentes entre proveedores de suministros subyacentes. Así, el proveedor puede haber contratado procesos con un tercero que no ofrezca las garantías o la confianza que el cliente desea, o que le sea desconocido. Recordemos que los servicios *cloud* en sí mismos son complejos y pueden unirse creando cadenas de suministros, dependiendo de distintos actores aspectos tan relevantes como la disponibilidad y la seguridad, y difuminándose las responsabilidades, las obligaciones de reparar y las garantías de rendimiento. De esta manera, debe prestarse especial atención a los roles y responsabilidades involucrados en la gestión de los datos y los riesgos de seguridad, y establecer una estrategia suficientemente flexible como para tratar con un entorno variable y en constante evolución.

Cuanto más inmersa esté la operativa de la empresa cliente en el entorno en la nube, mayor será su dependencia del proveedor. La pérdida de gobierno y de control sobre ciertas decisiones, como por ejemplo, aquellas decisiones sobre la destrucción de contenidos, son fruto de la cesión por parte del cliente al proveedor de cuestiones relacionadas con el tratamiento y la seguridad de los datos.

Así las cosas, el proveedor puede incumplir los acuerdos de nivel de servicio (ANS) u otros pactos inicialmente incluidos en el contrato, realizar políticas que puedan resultar perjudiciales para la estrategia empresarial y su consecución de objetivos, poner en riesgo la confidencialidad, integridad y disponibilidad de los contenidos; mermar el rendimiento informático y con ello la calidad del servicio que presta el cliente empresario, no cumplir con las obligaciones legales exigidas, etc. Además, según el tipo de servicio suscrito, el proveedor puede controlar el diseño, implementación, pruebas y monitorización del servicio distribuido por la empresa, como sucede, por ejemplo, con las plataformas como servicio (PaaS).

6.2.2. Riesgos técnicos

Un entorno de computación en la nube, como elemento complejo que es, está

---

por parte de ciertos usuarios, e implicó para muchos clientes la imposibilidad de recuperar sus datos o acceder a ellos, aun sin haber infringido, por su parte, normativa de *copyright* alguna. Actualmente, el software como servicio de almacenamiento de archivos *Mega*, sucesor de *Megaupload* y similar a *Dropbox* o *Box*, utiliza un sistema de cifrado que, según afirma el proveedor, imposibilita conocer la información que almacenan los clientes en sus servidores, y por tanto, les exime de responsabilidad en relación a esos contenidos. Sus condiciones del servicio están accesibles en línea: <https://mega.nz/#terms>. [Fecha de consulta: 27 de junio de 2016].

integrado por múltiples componentes físicos (hardware) y lógicos (software) que se crean y comunican entre sí mediante interfaces de programación. La seguridad global del entorno de la nube en su conjunto y de los servicios prestados a cliente dependerá, en buena parte, de la seguridad de cada uno de estos elementos individualmente considerados. Como los accesos se realizan a través de Internet, las medidas preventivas deberán extenderse a las conexiones a la propia red (por ejemplo, cortafuegos), a las implementadas por los navegadores y a las provistas en los sistemas de los dispositivos físicos (móviles o no). Todos estos elementos deberán someterse a una actualización sistemática, para que el cliente de computación en la nube disponga de las máximas garantías frente a eventuales amenazas externas. Por otro lado, la seguridad de los contenidos comprende tres aspectos esenciales: su confidencialidad[146], su integridad[147] y su disponibilidad[148], aspectos que serán tratados con detalle el capítulos posteriores[149].

Dentro de la nube existen diferentes grados de borrado, al igual que sucede en los ordenadores personales, y los datos pueden seguir disponibles más allá del plazo de duración del contrato, hasta que no se sobreescriban paulatinamente con datos más frescos por un cierto número de veces. Aunque la supresión total de los datos únicamente tiene lugar cuando se destruye el soporte físico que los almacena, este no es el mecanismo preferido por el proveedor de servicios *cloud*, puesto que supone un coste económico elevado (los datos se replican en múltiples dispositivos compartidos) y puede ser inviable económica y técnicamente llevarlo a la práctica en todos los centros de datos y para todos los clientes del proveedor[150].

Asimismo, la arquitectura de la nube es más susceptible de interceptación de datos en tránsito que los sistemas tradicionales, simplemente porque sus operaciones implican más tráfico de datos que aquellas: deben sincronizarse, replicarse,

146 "Confidencialidad". Propiedad de la información que garantiza que únicamente la conocen o tienen acceso a su contenido las personas autorizadas. (Definición propia).

147 "Integridad". Propiedad de la información que garantiza su corrección y completitud durante todo el ciclo de procesamiento de la información, es decir, que no han sido destruidos, alterados o modificados por personal no autorizado o de forma accidental desde que se migran a la nube o se crean en ella, hasta que finaliza la obligación contractual del proveedor de preservarlos en el sistema (los haya recuperado el cliente o no, según sea el caso), y puede procederse a su borrado progresivo o definitivo. (Definición propia).

148 "Disponibilidad". Propiedad de los datos que garantiza el acceso ininterrumpido a su contenido por parte del personal autorizado. (Definición propia).

149 Ver capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

150 Ver capítulo "Suspensión, modificación y extinción del contrato de servicios de computación en la nube".

distribuirse entre sus múltiples usuarios, etc. Sin embargo, el proveedor puede no ofrecer siempre las máximas garantías de seguridad para proteger información confidencial que circula en su entorno *cloud*.

La compartición de recursos caracteriza la computación en la nube de implementación pública, pero presenta riesgos. La mayoría de los componentes físicos subyacentes no están diseñados con sistemas que aseguren el aislamiento entre diferentes usuarios del mismo recurso, así que se instalan mecanismos técnicos encargados de realizar las segregaciones. Si estos sistemas están mal instalados, configurados o monitorizados, pueden producirse pérdidas de datos y accesos no autorizados, además de interrupciones del servicio mientras se reparan los componentes afectados. Asimismo, puesto que el hardware del proveedor contiene contenidos de múltiples clientes, la confiscación de dispositivos físicos por parte de las autoridades policiales o judiciales dentro de la investigación de un cliente de la nube puede suponer la retirada y/o puesta en compromiso de datos pertenecientes a otros usuarios o clientes no relacionados con tal investigación.

Los entornos de nube, como cualquier elemento informático conectado a la red, son potenciales objetivos de ataques maliciosos que podrían afectar a la seguridad de los datos, a la disponibilidad y a la integridad del sistema. Existe *malware* especialmente diseñado para detectar las vulnerabilidades y agredir los sistemas de computación en nube, sus capas de arquitectura o sus interfaces de control[151]. En atención al tipo de datos custodiados, hay que tener en cuenta que algunos de ellos son mucho más propensos a sufrir intentos de sustracción o accesos no autorizados, como los datos bancarios o gubernamentales.

Por su parte, los proveedores se protegen del abuso y mal uso de los servicios por parte de los clientes o de los usuarios finales. En servicios de infraestructura y plataforma (IaaS y PaaS) con registros de acceso poco restrictivos, los delincuentes informáticos pueden instalar su centro de operaciones para desarrollar *spams*[152] y

---

151 *"Malware"*. Contracción de las palabras inglesas "*malicious software"* que hace referencia a programas informáticos especialmente diseñados para dañar equipos informáticos o entorpecer su funcionamiento. Engloba, entre otras categorías, los *virus* ("infectan" otros archivos para modificarlos o dañarlos), los *troyanos* (se ocultan en el sistema huésped y desarrollan tareas sin que el usuario se percate), las *puertas traseras* (crean un acceso remoto al sistema para acceder a su información), los *botnets* (redes de ordenadores robot), o el *spyware* (destinado a captar información del ordenador huésped).

152 *"Spam"*. También llamado correo electrónico basura, son mensajes no solicitados, de contenido generalmente publicitario, y enviados de forma masiva e indiscriminada. Aunque el

demás códigos maliciosos[153]. Los softwares como servicio (SaaS) pueden utilizarse igualmente por los usuarios de manera ilícita, aprovechándose de las funcionalidades facilitadas por el proveedor para atentar contra la intimidad, la reputación o la propiedad intelectual de terceros. Por estos motivos, en los contratos de servicios *cloud* se establecen las llamadas "políticas de uso adecuado" o *PUAs*, en las que los proveedores se eximen de aquellas responsabilidades derivadas del comportamiento de sus clientes o usuarios[154].

No debemos olvidar la existencia de potenciales amenazas internas, donde son los propios usuarios de la organización suscriptora de servicios *cloud* (empleados o ex-empleados, empresas asociadas, asistentes técnicos, y otros actores con acceso a redes y datos) quienes actúan por error o desconocimiento, o con mala fe, pretenden perjudicar a la organización o beneficiarse de la información que se posee sobre datos empresariales y sus aplicaciones. En un entorno nube, se magnifica la capacidad de daño porque el acceso remoto a ciertas plataformas y archivos no monitorizados puede dificultar la identificación del infractor. Los proveedores de servicio deben facilitar a sus clientes los métodos de control de este tipo de amenazas, y es recomendable que los empleadores incluyan cláusulas de confidencialidad en los contratos laborales y establezcan procesos estrictos de notificación de altas y bajas en el sistema de acceso a las plataformas de computación en la nube.

Igualmente, pueden tener lugar usurpaciones de las claves de identificación de los usuarios, perpetradas por terceros ajenos a la organización o por otros usuarios no legitimados. Los puntos más vulnerables tienen lugar en los procedimientos de alta y baja de usuarios, en el propio mecanismo de acceso a la interfaz, y en el protocolo del usuario de custodia y renovación de sus claves. El acceso a cuentas y datos no autorizados pueden usarse en beneficio propio o para perjudicar económicamente a la entidad, y puede afectar a activos de información, a la

---

correo electrónico es la vía más utilizada, también puede llevarse a cabo mediante mensajería móvil, motores de búsqueda, foros y redes sociales, etc.

153 Por ejemplo, la red criminal que delinquía con ordenadores-zombie *Zeus Botnet* utilizaba los servicios de infraestructura de *Amazon EC2* para hospedar en la nube el servidor central de control y administración de las máquinas infectadas. Ver notícia en <http://www.zdnet.com/blog/security/zeus-crimeware-using-amazons-ec2-as-command-and-control-server/5110> y <http://www.securityfocus.com/brief/1046>. [Fecha de consulta: 6 de julio de 2016].

154 Ver apartado "Legalidad y adecuación de los contenidos alojados por el cliente. Las Políticas de Uso Adecuado y su control por el proveedor", en el capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

disponibilidad del sistema y a la reputación de la compañía.

Una de las características de la nube es la posibilidad del proveedor (y dependiendo del servicio *cloud*, también del cliente) de monitorizar el servicio, para calcular los recursos consumidos y para controlar potenciales usos no adecuados del servicio o la eficacia de las medidas de seguridad adoptadas. Aunque es un mecanismo necesario, no está exento de riesgo, porque los resultados recabados con estos exámenes pueden utilizarse para obtener información con intenciones desleales o ilegales, por ejemplo, para intentar el acceso a datos almacenados y demás información de la empresa cliente, como para detectar vulnerabilidades del sistema informático o errores humanos en el protocolo de seguridad.

A sabiendas de todo lo anterior, el cliente debe tomar consciencia de su responsabilidad, también en beneficio de sus propios activos, y solicitar información y asesoramiento al proveedor. Este, por su parte, debe ser capaz de comunicar los procedimientos tecnológicos y de actuación adecuados que el cliente debe y/o puede suscribir para maximizar la protección del entorno *cloud* y, consiguientemente, de sus contenidos digitales, en la medida de lo posible y siempre que con ello no ponga de manifiesto vulnerabilidades de seguridad del entorno.

6.2.3. Riesgos legales y retos jurídicos

Como uno de los principales debates en torno a la computación en la nube, el tema de la protección de datos de carácter personal ha sido objeto de múltiples estudios y debates (sobre todo dentro de los países de la Unión Europea). La materialización de leyes especialmente estrictas de protección de datos dentro del ámbito europeo puede resultar de difícil cumplimiento práctico dentro de los entornos de la nube, como veremos en posteriores capítulos dedicados expresamente a resolver dudas relacionadas con la privacidad[155].

En primer lugar, determinar a quién corresponden los roles que las leyes adjudican a responsables y encargados del tratamiento de datos personales puede resultar en algunos casos especialmente complicado, y, en otras ocasiones, los clientes no podrán asegurar el cumplimiento de las obligaciones por parte de los proveedores implicados. Una vez dentro de los sistemas del proveedor, el cliente pierde parte del control sobre los datos migrados y sobre el tratamiento al cual se

155 Ver capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

someterán, viéndose limitado a exigir información y a dar instrucciones en su papel de responsable, de acuerdo con el contrato que suscribe con el proveedor, quien cumplirá la función de encargado del tratamiento[156]. Por su parte, el proveedor puede que no notifique al cliente puestas en compromiso de los datos o infracciones de la normativa que hayan tenido lugar bajo su responsabilidad. Por imperativo legal, el empresario cliente de la nube será el responsable del tratamiento (y, como tal, pueden imponérsele sanciones administrativas de elevada cuantía, reclamaciones civiles o imputársele delitos penales), aunque en la práctica lo realice un proveedor. El proveedor únicamente ostentará el papel de responsable cuando tenga relación directa con el titular de los datos personales, y sea este quien se los facilite.

Los problemas derivados de la preservación de la privacidad y del cumplimiento de la normativa sobre protección de datos personales se intensifican cuando tienen lugar transferencias internacionales de datos a centros de procesamiento ubicados en países que carecen de normativa en la materia o cuya regulación es mucho más laxa. Como hemos mencionado con anterioridad, al utilizar entornos de nube no siempre se conoce el país en el cual están alojados los datos, ni en cuántos lugares existen réplicas de esos datos. Por eso es recomendable consultar a los proveedores sobre el régimen legal aplicado al tratamiento, almacenaje y procesamiento de los datos, y adecuarlo al marco jurídico europeo y nacional[157].

La nube también suscita dudas relacionadas con la propiedad intelectual[158]. Las condiciones impuestas por las diferentes licencias de software no son fácilmente comprobables por los clientes de la nube, puesto que en ocasiones no son siempre transparentes, utilizan términos ambiguos y pueden no hacer mención a su utilización dentro de este tipo de entornos, en los que el número de actores se multiplica. Por otra parte, el proveedor puede tener instalado software no legal, o el cliente descargarlo dentro de entornos virtuales *cloud* sin tener autorización para ello del titular del software. En otros casos, los datos almacenados por el cliente pueden ser objeto de derechos de autor de terceros. El que estén obtenidos o

156 En otras ocasiones, el proveedor podrá ser considerado responsable del tratamiento, como sucede en aquellos casos en los que se exceda de sus facultades como encargado o incumpla las instrucciones facilitadas por el cliente en su calidad de responsable, o cuando trate datos de carácter personal que le haya facilitado directamente el titular de esos datos.

157 La elección de proveedores cuyos centros de datos estén localizados dentro de países europeos o que garanticen con certificaciones el cumplimiento de la normativa de protección de datos europea será un buen mecanismo de salvaguarda para organizaciones que manejan datos personales.

158 Ver capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

descargados de forma legal o ilegal puede afectar indirectamente al proveedor que no restrinja estas descargas o que no establezca ningún tipo de cláusula de salvaguarda en el contrato con el cliente. En cuanto a la creación dentro de la nube de contenidos originales susceptibles de generar derechos de autor (por ejemplo, la creación de software mediante plataformas como servicio) u otros derechos de propiedad intelectual o industrial, estos trabajos pueden verse amenazados por cláusulas de cesión de derechos en favor del proveedor, camufladas en el contrato de suministro de servicios *cloud*. Por último, en cuanto a los contenidos migrados por el cliente que sean de su propiedad, encontramos cláusulas contractuales que esconden amplias cesiones por parte del cliente al proveedor, y que en ocasiones, exceden de los usos razonables que pueden esperarse de la prestación del concreto servicio *cloud*. En todo caso, deberá realizarse una pormenorizada clasificación de la categoría de los contenidos afectados, para poder determinar su titularidad y los cauces legales establecidos para su protección[159].

Dentro de este contexto, las normas aplicables son numerosas por su contenido (protección de datos personales, propiedad intelectual e industrial, competencia, protección de consumidores, regulación contractual, etc.). Todo ello plantea distintas cuestiones jurídicas, algunas de las cuales pretendemos abordar a través del presente trabajo, en el cual realizaremos propuestas de solución a los problemas legales que suscita la computación en la nube, y aclararemos algunas dudas no siempre resueltas con acierto a través del clausulado contractual o la normativa aplicable.

La redacción del contrato suscrito entre las partes será decisiva para solventar muchas de estas incógnitas. El clausulado del contrato entre proveedor de los servicios y cliente receptor de las capacidades informáticas establecerá, entre otros extremos: los niveles mínimos de calidad del servicio prestado (parte del acuerdo que se denomina acuerdo de nivel de servicio); los usos permitidos y/o prohibidos del servicio (políticas de uso adecuado o PUAs); el devengo de las cuotas y la determinación de su importe, así como de los costes de eventuales servicios accesorios; la distribución de riesgos y responsabilidades entre las partes; y eventuales compensaciones a cargo de la parte que incumpla con sus obligaciones contractuales.

159 Para un análisis más detallado de estas cuestiones, ver capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

Estos contratos se presentan al pequeño empresario a modo de condiciones generales predispuestas, y su suscripción es requisito imprescindible para la acceder a las capacidades informáticas ofrecidas. Sin embargo, muchos aspectos de estos contratos presentan problemas jurídicos. Entre otros, la propia naturaleza jurídica del contrato, la legalidad de ciertas prácticas relacionadas con la distribución de los riesgos entre las partes y la transparencia de la información facilitada sobre el funcionamiento del servicio, las contraprestaciones que subyacen bajo servicios ofertados como gratuitos, o la titularidad o destino de los contenidos que una parte pone a disposición de la otra, entre otros.

Como hemos observado, en el contrato de servicios se efectúa la distribución de responsabilidades entre proveedor, cliente, usuario final[160] y terceros[161]. En ocasiones, algunos proveedores abusarán de su poder de negociación, y en contratos con condiciones generales intentarán limitar y exonerar obligaciones que forman parte del cumplimiento de su deber de diligencia o *lex artis.* Por ello, las cláusulas potencialmente abusivas deberán analizarse dentro del marco de la normativa de protección a los consumidores y, en contratos suscritos entre empresas, en el marco de la legislación civil y mercantil aplicable, considerándose la posibilidad de la aplicación extensiva de la normativa de protección al consumidor en aquellos casos en los cuales el pequeño empresario se encuentre en una situación de indefensión similar[162].

Tras esta aproximación inicial al *Cloud Computing*, en la que hemos analizado sus características técnicas, sus ventajas y riesgos, y algunas de sus definiciones técnicas y jurídicas, en los capítulos siguientes analizaremos las principales implicaciones jurídicas (y especialmente mercantiles) que supone la suscripción de servicios de computación en la nube por parte del pequeño empresario. Como se ha delimitado en distintos apartados de este capítulo

160 Usuario final y cliente del proveedor pueden no coincidir. El usuario final será el eslabón último de una cadena de contratos de suministros de computación en nube más o menos larga, como un empleado de la organización suscriptora del contrato de servicios *cloud* o un consumidor de los bienes y servicios ofrecidos por esta. Ver capítulo "Elementos subjetivos del contrato de servicios de computación en la nube".

161 Estos terceros pueden ser otros proveedores, sujetos de derechos de propiedad intelectual o autoridades.

162 Ver apartado "Breve reflexión sobre la aplicación extensiva de las normas y criterios de las cláusulas abusivas al pequeño empresario. Extensión al ámbito de la contratación de servicios de *Cloud Computing",* en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

introductorio, el objeto de esta tesis se centra en los aspectos jurídico-mercantiles de la suscripción de contratos de servicios de nube pública por pequeños empresarios, la cual generalmente corresponderá con servicios de software, y en las eventuales aplicaciones y problemática de estos servicios cuando se suscriben por pequeños empresarios del sector turístico.

Capítulo Segundo

OBJETO, NATURALEZA JURÍDICA Y CARACTERÍSTICAS DEL CONTRATO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE PÚBLICA

1.- INTRODUCCIÓN

Como hemos expuesto, la computación en la nube permite abastecerse de recursos informáticos (capacidades de almacenamiento y procesamiento, aplicaciones informáticas con diversas funcionalidades, máquinas virtuales, plataformas para desarrollar software, etc.) de una forma rápida, sencilla y eficiente[1]. Presenta múltiples ventajas para cualesquiera usuarios, entre los que se encuentra el pequeño empresario, en quien centramos nuestro trabajo[2].

1 Ver capítulo "Concepto y características técnicas de la computación en la nube".

2 Como se ha dicho, este trabajo se centra en la contratación de servicios de computación en la nube por parte de microempresarios, pequeños y medianos empresarios puesto que, por sus dimensiones, carecen de poder de negociación y por ello suscriben condiciones generales predispuestas por el proveedor, con lo cual, en principio, no pueden beneficiarse de la protección ante comportamientos abusivos que ampara al consumidor. Englobamos este conjunto de empresarios bajo el concepto amplio "pequeño empresario".

CAPÍTULO SEGUNDO

De acuerdo con lo analizado en el capítulo precedente, se ponen de manifiesto diferencias entre las prestaciones que pueden ser objeto del contrato de computación en la nube pública. En este sentido, es obvio que existen distinciones entre los modelos de servicio *cloud* que prestan recursos de infraestructura (IaaS), plataforma (PaaS) y aplicaciones (SaaS), e incluso entre servicios que podrían compartir la misma categoría, especialmente en el caso del software como servicio (SaaS).

Esta heterogeneidad, al contrario de lo que pueda parecer, no alcanza únicamente a aspectos técnicos o prácticos, sino que jurídicamente desemboca en diferencias en la relación negocial que pueden ser relevantes en la ejecución del contrato entre las partes. Especialmente, en lo referente a la distribución de las tareas de gestión de los recursos y la seguridad de los datos implicados y, consecuentemente, en la gradación de los deberes de diligencia entre ambas partes[3]. Sin embargo, todos los contratos presentan caracteres comunes que nos permiten identificarlos como contratos de computación en la nube pública. En esencia, todos los contratos de *Cloud Computing* implican la puesta a disposición de recursos informáticos a través de Internet a petición del cliente, permitiéndole procesar, transportar y/o almacenar su propia información digital gracias a las herramientas y capacidades facilitadas por el proveedor, sin necesidad de adquirir, actualizar o mantener hardware o software[4]. Dedicaremos el presente capítulo a estudiar las características que definen los contratos de nube pública, así como sus diferentes objetos.

Como puede deducirse de lo anterior, tal diversidad de contenidos y configuraciones técnicas dificulta la determinación de la naturaleza jurídica del contrato. En principio, los contratos de servicios de nube pública pueden mostrar semejanzas con otras categorías de contratos, como el *Hosting* o el *Outsourcing*, puesto que estos últimos consisten en la prestación de servicios similares a través de técnicas antecesoras de los entornos *cloud*, como se ha observado en el capítulo anterior[5]. Igualmente, estos contratos exhiben aspectos coincidentes con otras figuras

3 Ver Figura 2, en el capítulo "Concepto y características técnicas de la computación en la nube".

4 Se enumeran tres de las utilidades de los recursos *cloud* para el cliente, aunque, como se ha visto en el capítulo anterior, esta lista no es una lista cerrada. A modo de ejemplo, los recursos sirven también para establecer comunicaciones entre usuarios, proporcionar acceso a bases de datos, etc.

5 Para observar las diferencias técnicas entre *Outsourcing, Hosting* y *Cloud Computing*, ver apartado "Qué no es *Cloud Computing*", en el capítulo "Concepto y características técnicas de la

jurídicas clásicas, como el suministro y el depósito[6]. En este capítulo observaremos las semejanzas y diferencias entre estas figuras jurídicas con el fin de establecer una propuesta en cuanto a la naturaleza jurídica del contrato de *Cloud Computing*.

Queremos avanzar que, como resultado de nuestro análisis sobre la naturaleza jurídica del contrato de computación en la nube, concluimos que este se presenta como figura autónoma, atípica y compleja, distinta de aquellas ya existentes en nuestro ordenamiento jurídico, tal y como en su momento sucedió con el *Hosting*[7]. Ello es así porque del contrato de servicios de computación en la nube derivan una serie de obligaciones para las partes que le son propias e inherentes en atención a su naturaleza. Sin embargo, estas obligaciones adoptan diferente grado de exigencia y de carácter vinculante, atendiendo a aspectos como la modalidad de implementación en el sistema informático del cliente, los recursos computacionales que conforman el objeto del contrato, la existencia o no de contraprestación dineraria, la distribución contractual de riesgos entre las partes, si va destinado a clientes profesionales o a consumidores finales, etc.[8] En este capítulo expondremos los fundamentos que consideramos que sustentan las anteriores afirmaciones.

Para acabar con esta introducción, queremos recordar que este trabajo se centra en la contratación de servicios de nube pública por el pequeño empresario a través de condiciones generales de la contratación y, especialmente, en los aspectos mercantiles de esta relación jurídica. Todo ello sin perjuicio de que, en este capítulo, se realicen referencias a otros modelos de implementación, y de que algunas conclusiones sean extensibles también a la contratación con consumidores y a contratos negociados.

2.- OBJETO DE LOS CONTRATOS DE COMPUTACIÓN EN LA NUBE

Los servicios de computación en la nube pública se caracterizan por estar disponibles para cualquier cliente, a diferencia de lo que sucede en entornos de nube

computación en la nube".

6 Aunque estas no se conforman, por definición, de un objeto tecnológico.

7 En relación a la calificación jurídica del *Hosting* como contrato atípico, nos remitimos a YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet, Hosting y búsqueda*, Navarra, 1ª edición, 2012, pág. 314.

8 Como hemos observado en el capítulo anterior, las modalidades de implementación de entornos en la nube son: nube privada, nube comunitaria, nube híbrida y nube pública.

privada o comunitaria, en los que el conjunto de recursos que recibe el cliente no se comparte con ningún otro usuario, o únicamente están disponibles para uno o varios clientes[9]. Por ello, es un rasgo definidor de la mayoría de servicios de nube pública su oferta y comercialización destinada al pequeño empresario o a consumidores a través de cláusulas predispuestas por el proveedor en su sitio web, a las cuales el cliente debe adherirse para acceder a la prestación[10].

Aunque debido a su presentación como contratos de adhesión pueden parecer contratos con contenido homogéneo, debemos tener presente que no existe un tipo único y uniforme de contrato de *Cloud Computing*. Los diferentes modelos de servicio descritos por el *National Institute of Standards and Technology* (NIST)[11] pueden servir de referencia a la hora de clasificar los diferentes objetos que en cada caso integrarán el contrato de nube pública[12].

A grandes rasgos, y como hemos expuesto en el capítulo precedente, podemos hablar de la existencia de tres distintos tipos de servicio: infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS). A través del contrato de infraestructura como servicio (IaaS), el cliente puede hacer uso de capacidades que provienen de máquinas virtuales, tales como procesamiento, almacenamiento o entornos virtuales de red[13]. Por otro lado, cuando se contrata un modelo de plataforma como servicio, se permite al cliente crear todo o parte del ciclo de vida de un programa informático (diseñar, desplegar, probar, administrar, etc.)

9 Ver apartado "Los modelos de implementación de la nube", en el capítulo "Concepto y características técnicas de la computación en la nube".

10 En este trabajo, nos centraremos en los contratos suscritos por pequeños empresarios, y únicamente apuntaremos de forma puntual ciertas cuestiones relevantes en relación a los consumidores.

11 El NIST realiza una definición técnica de los servicios de infraestructura como servicio, plataforma como servicio y software como servicio, recogida en el capítulo "Concepto y características técnicas de la computación en la nube", concretamente en el apartado "Los modelos de servicio en la nube".

12 En nuestra opinión, si bien las características relativas a la monitorización de los datos por parte del proveedor y la compartición de recursos definen los servicios de computación en la nube en su vertiente técnica, los efectos jurídicos que se derivan de ellas no son suficientemente relevantes como para considerarlos parte integrante del objeto contractual común a todos los contratos de computación en la nube.

13 Este modelo de servicios suele contratarse por clientes con conocimientos avanzados de informática, departamentos de empresas con elevadas necesidades de capacidad computacional, o por desarrolladores de software que los utilizarán como soporte añadido a servicios de plataforma (PaaS). Algunos ejemplos de estos servicios son *Microsoft Azure* o *Google App Engine*.

utilizando diferentes lenguajes, herramientas y entornos que le proporciona el proveedor[14]. Pero sin duda alguna, el más extendido entre pequeños empresarios (y también consumidores) es el software como servicio (SaaS), con el cual el cliente puede hacer un uso fácil, útil y cómodo de las funcionalidades que le permiten las aplicaciones informáticas proporcionadas por el proveedor, quien conserva en sus sistemas la parte lógica y los datos que el cliente introduce en el software[15].

Cada categoría de servicio *cloud* (infraestructura como servicio, plataforma como servicio y software como servicio) viene determinada por los recursos computacionales que el proveedor pone a disposición del cliente, y el objeto contractual se adecuará a las particularidades de esos recursos computacionales[16]. En cuanto al aspecto técnico, cada uno de estos servicios se asocia también a las diferentes capas sobre las cuales se sustenta la arquitectura de la computación en la nube[17]. Jurídicamente, la relevancia de la distinción entre los objetos contractuales radica básicamente en la diferente distribución de obligaciones y responsabilidades entre proveedor y cliente, dependiendo de las opciones de control sobre el recurso que se ceden al cliente de acuerdo con lo publicitado y con lo estipulado en las condiciones generales[18].

Sin embargo, aunque estas tres categorías de servicios parecen claramente

---

14 Este modelo de servicios suele contratarse por desarrolladores profesionales de programas informáticos y con conocimientos avanzados de informática. Algunos ejemplos de estos servicios son *Amazon Web Services*, *GoGrid* o *Google Compute Engine*.

15 Este modelo es el más conocido y utilizado por pequeñas y medianas empresas y por consumidores. Como ejemplos de proveedor SaaS cuyos servicios se dirigen a empresas, podemos mencionar a *Google G-Suite*, *Dropbox para empresas, Microsoft Office 365* o *Salesforce.* En cuanto a softwares como servicio dirigidos a consumidores finales, podemos mencionar *Google Docs* o *Gmail.* Y como ejemplos de software como servicio orientados a empresas turísticas, *Hotelogix* o los *PMS (Property Management System) Cloud* de los proveedores *Engisoft* o *Quonext.*

16 Para observar de manera ilustrativa los recursos suministrados en cada una de las modalidades de servicio, ver el apartado "Los modelos de servicio en la nube" del capítulo "Concepto y características técnicas de la computación en la nube".

17 Ver apartado "La arquitectura en capas de la nube y sus principales modelos de negocio", en el capítulo "Concepto y características técnicas de la computación en la nube".

18 Por ejemplo, un servicio *cloud* de infraestructura de almacenamiento puede permitir al cliente configurar ciertos aspectos de seguridad, como controles de acceso a los datos. De esta manera, el deber de diligencia entre proveedor y cliente en relación al control de esos accesos, sobre los cuales el cliente tiene parte del control, quedará distribuido entre ambas partes, o incluso, puede llegar a exonerar al proveedor, dependiendo del tipo de incidente acontecido y de lo estipulado contractualmente. Ver Figura 2, en el capítulo "Concepto y características técnicas de la computación en la nube".

diferenciables, la práctica tanto contractual como técnica nos lleva, en ocasiones, a prestaciones en las que se combinan diferentes opciones (por ejemplo, se ofertan servicios de infraestructura y redes virtuales para desarrolladores[19] o softwares como servicio que permiten el almacenamiento remoto de información[20]) y en las que es difícil realizar una distinción clara y absoluta entre los tres tipos de servicios.

Por otro lado, como se ha mencionado, existen otras categorías adicionales de servicios que pueden prestarse a través de contratos de nube pública y que se sustentarán sobre equipos hardware del proveedor, aunque pueden pertenecer a diferentes capas[21]. Sucede con la puesta a disposición de bases de datos (*Database as a Service*)[22], servicios de correo electrónico o comunicaciones (*Email as a Service*), sistemas integrados de seguridad[23] (*Security as a Service*), etc.[24] Todo ello complica aún más la determinación de un objeto común de los contratos de *Cloud Computing,* teniendo que reducirlo al común denominador de los recursos de computación.

Teniendo en consideración lo anterior, y como resultado de nuestro estudio, consideramos apropiado hablar de un objeto contractual predicable de los contratos de computación en la nube, cuyo núcleo común sería la contratación de recursos computacionales en un volumen escalable, a los cuales el cliente accede a través de Internet, y que gestionará a modo de autoservicio. El contenido contractual concreto dependerá del servicio suscrito en cada caso particular, teniendo en cuenta que un

19 Por ejemplo, el servicio de plataforma de *Microsoft Azure* puede utilizarse en combinación con redes virtuales o máquinas virtuales.

20 Por ejemplo, los software como servicio (SaaS) *Dropbox para empresas*, *Box* o *iCloud* suministran una aplicación que permite guardar datos en los equipos del proveedor, remitidos desde diferentes dispositivos del cliente con conexión a Internet.

21 Ver apartado"Otros modelos de servicio", en el capítulo "Concepto y características técnicas de la computación en la nube".

22 Nos referimos a servicios que permiten desarrollar y administrar bases de datos. Como ejemplo, los servicios *SQL Azure* del proveedor *Microsoft,* o *Database.com* del proveedor *Salesforce.*

23 Las denominadas "*suites* de seguridad en la nube" son softwares como servicio (SaaS) que integran una suma de diferentes programas de seguridad (antivirus, antiespía, cortafuegos, copia de seguridad, etc.) que se instalan conjuntamente en el sistema del cliente y se actualizan de forma automática. Como ejemplos de proveedores de *suites* de seguridad podemos mencionar *Infospyware*, *Bitdefender* o *Avira*.

24 Todos estas categorías de servicios se identifican como servicios *cloud* emergentes por el estándar ISO/IEC 17788:2014, elaborado por la *International Organization for Standardization* y la *International Electrotechnical Commission.* Estas figuras pueden reconducirse a la categoría de software como servicio (SaaS). *ISO/IEC 17788:2014* [en línea]. Disponible en: <http://www.iso.org/iso/catalogue_detail?csnumber=60544>. [Fecha de consulta: 10 de abril de 2017].

mismo contrato puede combinar uno o varios modelos de servicio, y que su configuración dependerá también de la política comercial de cada proveedor.

De ese concreto contenido contractual se derivarán distintas consecuencias jurídicas. En particular, diferentes derechos y obligaciones, los cuales serán objeto de análisis en capítulos posteriores de este mismo trabajo.

3.- FIGURAS AFINES AL CONTRATO DE COMPUTACIÓN EN LA NUBE

A continuación, analizaremos algunas figuras contractuales que pueden parecer afines al contrato de computación en la nube, concretamente: el *Outsourcing*, el *Hosting,* el suministro, el depósito y las licencias de uso no personalizadas de software, para así establecer sus principales características y sus similitudes y diferencias, con el objetivo último de determinar la naturaleza y la noción jurídica del contrato de *Cloud Computing.*

3.1.- El contrato de *Outsourcing* informático

El contrato de *Outsourcing* se ha definido como aquel contrato mediante el cual las actividades informáticas de una empresa pasan a ser desarrolladas por un proveedor (en principio ajeno a la primera), a cambio de un precio y por un tiempo acordado[25], configurándose como un contrato de tracto sucesivo[26].

En ambos contratos, *Outsourcing* y computación en la nube, los sistemas

25 APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática. Introducción al Outsourcing de los sistemas de información*, 1ª edición, Granada, 2002, pág. 23. DE CARLOS BERTRÁN define el *Outsourcing* como "la contratación por una sociedad de uno o varios proveedores externos para la prestación, mediante el empleo de activos ajenos a la estructura interna de la sociedad, de un servicio que anteriormente desarrollaba un departamento interno de la misma". DE CARLOS BERTRÁN, José Manuel; "El *Outsourcing* como técnica de gestión alternativa y su regulación contractual", *Derecho de los negocios,* núm. 91, Madrid, 1999, pág. 11. El autor DEL PESO NAVARRO, por su parte, define el *Outsourcing* informático como "la subcontratación de todo o parte del trabajo informático mediante una empresa externa que se integra en la estrategia de la empresa y busca diseñar una solución a los problemas existentes". DEL PESO NAVARRO, Emilio, "Contratación global de los servicios informáticos: el contrato de *Outsourcing*", *Encuentros sobre Informática y Derecho de la Universidad Pontificia de Comillas* 1994-1995, Pamplona, 1995, pág. 112.

26 APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática..., op. cit.,* pág. 38. VAQUERO PINTO, María José; "Contratos de prestación de servicios y realización de obras", *Tratado de contratos*, Vol. III, 1ª edición, Valencia, 2009, pág. 3422.

informáticos de un tercer proveedor permiten procesar y almacenar datos del empresario cliente, liberándose este de las actividades informáticas y pudiendo centrar su atención en su propia actividad de negocio[27]. Sin embargo, podemos observar algunas diferencias entre ambos contratos de externalización informática. A continuación, nos detendremos en las que, a nuestro parecer y coincidiendo con otros autores, son las principales[28].

En primer lugar, a diferencia del *Outsourcing*, la computación en la nube se caracteriza por el papel activo del cliente, quien se encarga de sus propias tareas informáticas (procesa sus datos, los almacena, etc.), utilizando para ello los recursos que le facilita el proveedor, gracias a la configuración a modo de autoservicio, característica del *cloud*. El proveedor, por su parte, no elige qué datos almacena o cómo los procesa, sino que únicamente realiza funciones de mantenimiento, seguridad y accesibilidad para permitir al cliente el uso eficaz de los recursos y su aplicación sobre los contenidos informáticos que maneja. El acceso a los datos empresariales por parte del proveedor, en principio, es meramente instrumental, puesto que es el propio cliente quien los procesa utilizando para ello los recursos que le son facilitados. El proveedor, por su parte, asumirá diferentes grados de compromiso en relación a su custodia, de acuerdo con lo que establezcan las cláusulas contractuales y al modelo de servicio contratado[29], y el cliente tendrá un margen reducido en cuanto a la imposición de condiciones o instrucciones sobre la gestión de los datos migrados al proveedor[30]. En el *Outsourcing*, en cambio, el proveedor tiene acceso a datos relevantes de la empresa, y los procesará de acuerdo con las instrucciones recibidas por el cliente y con las estipulaciones contractuales[31].

---

27 En cuanto a sus aspectos técnicos, ver subapartado dedicado al *Outsourcing*, en el apartado "Qué no es *Cloud Computing*", en el capítulo "Concepto y características técnicas de la computación en la nube".

28 KUAN HON, W; MILLARD, C, "Control, Security, and Risk in the Cloud", *Cloud Computing Law,* (Ed. Christopher Millard), 1ª edición, Oxford, 2013, pág. 31.

29 Respecto de las diferencias entre los diferentes modelos de servicio, ver Figura 2, en el capítulo "Concepto y características técnicas de la computación en la nube".

30 Generalmente, el proveedor afirma que el cliente es el encargado de procesar los datos, con lo cual únicamente se suele comprometer a cumplir con ciertos aspectos relacionados con la custodia de los datos y a seguir las instrucciones relacionadas con la normativa de protección de datos personales. Ver capítulos "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal" y "Obligaciones y Responsabilidades de las partes del contrato de computación en la nube".

31 Por ejemplo, la externalización de tareas relacionadas con las nóminas de los empleados de la

En segundo lugar, en el *Outsourcing* el proveedor diseña soluciones tecnológicas personalizadas y ajustadas a las concretas necesidades del empresario cliente, y ambos se someten a la negociación de los diferentes aspectos e instrucciones que regularán la concreta prestación del servicio[32]. Posteriormente, si lo considera necesario, el prestador del servicio subcontratará a otros proveedores para que le ayuden con la prestación debida. En cambio, la mayoría de servicios del *Cloud Computing,* y más concretamente aquellos sustentados por la modalidad de nube pública, se presentan estandarizados y listos para ser consumidos en masa, con lo cual el cliente puede beneficiarse de las economías de escala, aunque deberá compartir con otros usuarios el entorno en el cual se sustentan[33]. Dado que el servicio *cloud* viene diseñado de antemano para proporcionar recursos de manera escalable y elástica a múltiples usuarios a la vez, la subcontratación por parte del proveedor generalmente ha tenido lugar de manera previa a la contratación con el cliente[34].

Otra diferencia relevante entre los sistemas de *Outsourcing* y los sistemas *cloud* es la relativa al control y el conocimiento del cliente sobre el servicio. El cliente de *Outsourcing* tiene conocimiento detallado de todos los recursos informáticos involucrados en la prestación, y es quien dará instrucciones al proveedor sobre su uso y gestión, a través de un contrato negociado y personalizado. De este modo, confía al proveedor el procesamiento de ciertas categorías de datos, en un contrato *intuitu personae*[35].

En la computación en la nube, la tarea de introducir los datos en el sistema y procesarlos recae sobre el cliente. Consecuentemente, aunque existen diferentes grados de control del cliente sobre esos datos dependiendo del tipo de servicio y del

---

empresa cliente.

32 Semejanza que, por otro lado, comparte el *Outsourcing* con la modalidad de implementación privada del *Cloud Computing* (o nube privada).

33 Se trata de la agrupación o multitenencia de recursos, característica del *Cloud Computing* que permite al proveedor la asignación dinámica y elástica de recursos en respuesta inmediata a la demanda de cada uno de los clientes. Los datos de cada uno de los clientes están aislados unos de otros a través de sistemas lógicos, pero comparten el mismo entorno hardware. Ver subapartado "agrupación de recursos y *multi-tenancy*", en el apartado "Definición y características técnicas según el *National Institute of Standards and Technology* (NIST) del capítulo "Concepto y características técnicas de la computación en la nube".

34 De este modo, se produce un cambio en la secuencia de eventos que integran la preparación de la prestación. KUAN HON, W; MILLARD, C, "Control, Security, and Risk...", *op. cit.*, pág. 31.

35 APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática..., op. cit.,* pág.58.

concreto recurso de que se trate, el cliente a menudo desconocerá muchos de los aspectos relacionados con el servicio, como las subcontrataciones a terceras empresas efectuadas por el proveedor, la infraestructura física y lógica involucrada en la prestación del servicio, la identidad de otros usuarios con quien comparte los recursos en "multitenencia" o la ubicación exacta de los centros de datos donde se almacena la información que ha migrado. Aunque los clientes de servicios *cloud* de infraestructura tendrán un control más amplio sobre los recursos que los clientes de servicios *cloud* de plataforma o software, el grado de conocimiento y control sobre el servicio es muy inferior al del cliente que contrata un *Outsourcing* informático[36].

Por último, podemos distinguir el *Outsourcing* de la computación en la nube en que gran parte de los servicios de *Cloud Computing*, especialmente los de software como servicio, pueden ser contratados por consumidores, a través de los mencionados contratos de adhesión y la configuración del *cloud* a modo de autoservicio[37]. Esta posibilidad no tiene cabida en el *Outsourcing,* debido a su naturaleza estrictamente empresarial y compleja[38].

Para finalizar concluimos que, aunque el *Outsourcing* y el *Cloud Computing* son, en nuestra opinión y coincidiendo con otros autores, contratos de arrendamiento de servicios, sus muchas diferencias impiden considerarlos equivalentes[39].

---

36 Ver la "Figura 2" sobre los distintos modelos de servicio, en el capítulo "Concepto y características técnicas de la computación en la nube".

37 En cuanto al autoservicio como característica de la computación en la nube, recordemos que los servicios *cloud* se prestan mediante mecanismos automatizados (a menudo, a través de una interfaz diseñada a tal efecto), permitiendo al cliente administrar su propio suministro de forma ágil a través de Internet, todo ello a modo de autoservicio y con la mínima intervención del proveedor. Ver subapartado "autoservicio bajo demanda", en el apartado "Definición y características técnicas según el National Institute of Standards and Technology (NIST)" del capítulo "Concepto y características técnicas de la computación en la nube".

38 APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática..., op. cit.,* págs. 33, 55.

39 En opinión de APARICIO VAQUERO, con quien coincidimos, el contrato de *Outsourcing* (informático global simple) se corresponde con el contrato de arrendamiento de servicios. APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática..., op. cit.,* pág. 69 y ss. Por su parte, VAQUERO PINTO afirma que el *Outsoutcing* o externalización de funciones de la empresa (entre ellas, la gestión informática) no puede identificarse con un tipo contractual concreto, debido a su complejidad y diversidad. VAQUERO PINTO, María José, *Contratos de servicios,* pág. 939. La jurisprudencia, en cambio, en unas ocasiones lo ha identificado como contrato de arrendamiento de obra, atendiendo a la personalización del servicio (Sentencia de la Audiencia Provincial de Sevilla de 30 de septiembre de 2002; Sentencia del Tribunal Supremo de

3.2.- El contrato de *Hosting* y de alojamiento de datos por cuenta de terceros

En el contrato de *Hosting,* el prestador posibilita el almacenamiento de datos asignando hardware físico o virtual al cliente, junto con una capacidad limitada y definida cuantitativamente, permitiendo el acceso a estos a través de Internet[40]. Este hardware físico o virtual procede de un centro de datos compartimentado e independiente de otros soportes de almacenamiento[41]. A continuación, diferenciaremos entre el contrato de *Hosting* y el contrato de servicios *cloud* a partir de algunos de sus aspectos jurídicos.

Antes de proceder a la distinción entre contratos de computación en la nube y contratos de *Hosting*, nos detendremos en el análisis relativo a si el *Hosting* y el alojamiento de datos se refieren al mismo contenido contractual. En este sentido, el art. 14 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), y de donde proviene el art. 16 de nuestra Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, tradujo el concepto *Hosting* de su versión original en inglés al español utilizando la expresión "alojamiento de datos".

La expresión "alojamiento de datos" se recoge también en la Propuesta de Código Mercantil, cuya tramitación está paralizada en la actualidad, que en su artículo 532-12 define el alojamiento de datos como aquel contrato en el que "el prestador, a cambio del pago de una remuneración, se obliga frente al cliente a poner a su disposición una determinada capacidad de almacenamiento en un sistema de información bajo su control, a conservar los datos o la información almacenados, así como, en su caso, a permitir el acceso de terceros a los mismos en las condiciones pactadas en el contrato o, en su defecto, conforme a lo previsto en el presente Código o en disposiciones especiales", y comprende, entre las obligaciones principales del prestador "poner a disposición del cliente la capacidad de almacenamiento pactada en un sistema de información bajo su control, así

---

21 de julio de 2003, Sentencia de Audiencia Provincial de Cantabria, de 15 de octubre de 2004, Sentencia de la Audiencia Provincial de Badajoz, de 30 de junio de 2005); mientras que en otras ocasiones lo ha considerado arrendamiento de servicios (SAP Madrid de 7 de junio de 2004, STSJ del Principado de Asturias de 24 de febrero de 2006).

40 YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet..., op. cit.,* pág. 319.

41 En cuanto a la distinción técnica con la computación en la nube, ver apartado "Qué no es *Cloud Computing: el Hosting*", en el capítulo "Concepto y características técnicas de la computación en la nube".

como permitir el acceso del cliente a dicho sistema de información para el alojamiento, la recuperación, el manejo o la cancelación de los datos o la información almacenados. (...) Cuando así se haya pactado,(...) permitir el acceso de terceros a la información alojada a través de la red de comunicaciones electrónicas, previa disposición de los mecanismos de direccionamiento necesarios, (...) y a conservar los datos o la información alojados por el cliente y mantener su integridad"[42]. Esta definición abarca tanto los contratos de hospedaje de página web, puesto que en estos se permite el acceso a terceros a la página web creada en el entorno virtual que el proveedor ha facilitado al cliente, como los contratos de disco duro virtual, en los que la información alojada en el servidor del prestador no se publica en Internet, y que son predecesores de los contratos de computación en la nube de almacenamiento remoto[43]. Por tanto, consideramos que el sentido amplio que concede la Propuesta de Código Mercantil al contrato de "alojamiento de datos" alcanzaría no solo a los contratos de hospedaje de páginas web, sino también a aquellos contratos de computación en la nube que implican el almacenamiento remoto de contenidos digitales del cliente y que se corresponden con el concepto y las características de *Cloud Computing* definidos por el NIST.

Así, se ha afirmado que "en puridad, el alojamiento de datos es tan solo uno de los elementos esenciales del *Hosting*", debiendo entenderse el contrato de *Hosting* como "aquel contrato por el cual el prestador se obliga a: i) posibilitar el almacenamiento de información (hasta una determinada capacidad fijada en el propio contrato) en un soporte informático, ii) conservar los datos; y iii) hacerlos accesibles a través

42 Siguiendo con el mismo texto, las disposiciones de los contratos de servicio de comunicación electrónica serían aplicables también al contrato de alojamiento remoto de datos (excepto lo dispuesto sobre responsabilidad del prestador de servicios de comunicaciones electrónicas por incumplimiento), por imperativo del artículo 532-1 y cuando no se contradigan con el objeto del servicio: "Salvo en lo que resulte incompatible con su contenido o finalidad, serán de aplicación al contrato de alojamiento de datos y a la obligación de realizar copia temporal las disposiciones relativas al contrato de servicio de comunicación electrónica". Estas disposiciones recogen, entre otras obligaciones del proveedor, la obligación de "mantener el secreto de las comunicaciones" y de la obligación del cliente de "pagar al prestador la remuneración pactada, en el momento y la forma previstos (...) b) a hacer uso del servicio conforme a las condiciones previstas en el contrato, y en cualquier caso con respeto a los derechos de terceros, la ley y el orden público; c) a custodiar y mantener el secreto de cualesquiera instrumentos o medidas de seguridad" (art. 532 y siguientes de la Propuesta). Para un estudio más detallado del contrato de alojamiento de datos en la Propuesta de Código Mercantil, nos remitimos a ASENSI MERÁS, Altea, "Los contratos para las comunicaciones electrónicas", *Estudios sobre el futuro Código Mercantil.* Libro *Homenaje al Profesor Rafael Illescas Ortiz*, Madrid, 2015, págs. 1204 y ss.

43 Así, el contrato de hospedaje de página web puede incluir, además del alojamiento de información del cliente en e servidor del proveedor y el acceso a través de la Red a la página web que ha creado, otros servicios accesorios: cuentas de correo electrónico, copias de seguridad de la información alojada, etc. SÁNCHEZ LERÍA, Reyes; "Contrato de hospedaje en página web: estructura contractual básica y protección de los usuarios", *Revista de contratación electrónica*, núm. 61, 2005, págs 4 y 5.

de la red global que constituye Internet"[44]. En este sentido, por nuestra parte, coincidimos con la opinión estos autores en que existe un deber de custodia de los datos por parte del proveedor, y en que el almacenamiento de información del cliente en el servidor del proveedor implica el deber de custodiar esa información de manera segura, conservando su confidencialidad, integridad y disponibilidad, con lo cual este deber de custodia se configuraría como una obligación inherente al contrato de *Hosting*[45]. Otra postura doctrinal se refiere al deber de custodia de la información como una obligación accesoria y no como un deber esencial del contrato de *Hosting,* especialmente respecto del hospedaje de página web, al entenderse en este caso que el fin último del contrato es la presencia del sitio web en Internet[46].

En nuestra opinión, si bien el concepto de alojamiento de datos recogido por la Propuesta de Código Mercantil puede abarcar algunos contratos de computación en la nube que impliquen el alojamiento remoto de contenidos digitales del cliente, lo cierto es que el contrato de computación en la nube suele abarcar elementos distintos o añadidos al alojamiento remoto de información, de los cuales carece el contrato de *Hosting*. Entre estos elementos cabe destacar, en primer lugar, la ya mencionada existencia de un objeto más amplio del contrato, pudiendo consistir en funcionalidades facilitadas por aplicaciones informáticas, en redes virtuales o en plataformas de desarrollo de software, sin tener que corresponderse estrictamente

44 Sin embargo, a diferencia de lo que opina en autor, nos decantamos por considerar el contrato de *Hosting* como un contrato de servicios y no como un arrendamiento de obra, ya que creemos que la gran mayoría de las obligaciones a las cuales se compromete el proveedor son de puesta a disposición del cliente de mecanismos que le permitan acceder a los recursos informáticos (es decir, obligaciones de medios), y no van vinculadas a la obtención de un resultado final. Cosa distinta es el contrato de diseño de página web, que sí consiste en la entrega de una obra que presenta determinadas características concretas y adaptadas a los requisitos del cliente, como resultado del contrato. YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet..., op. cit.*, págs. 315 a 316.

45 YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet..., op. cit.*, págs. 315 a 316.

46 SÁNCHEZ LERÍA establece que el prestador de servicios del contrato de *Hosting* se obliga a "la cesión de uso de un espacio de memoria de su servidor para que (...) el cliente almacene allí su sitio web, al mismo tiempo que conecta el servidor a una red de telecomunicaciones de tal forma que la información alojada tenga acceso a Internet". Afirma la autora que, al ser la finalidad última del contrato la presencia del sitio web en Internet, la obligación de custodia se configura como accesoria, no es aplicable al *Hosting* el régimen jurídico del contrato de depósito. SÁNCHEZ LERÍA, Reyes, *El contrato de hospedaje de página web*, 1ª edición, Valencia, 2011, pág. 69 y ss. Para otras definiciones del contrato de *Hosting de página web*, nos remitimos también a LLANEZA GONZÁLEZ, Paloma, *E-contratos,* 1ª edición, Barcelona, 2004, pág. 96, y DE MIGUEL ASENSIO, Miguel A, *Derecho Privado de Internet,* 5ª edición, 2015, págs. 99 a 103.

con el almacenamiento remoto de datos del cliente. En segundo lugar, en cuanto a las obligaciones esenciales de las partes, también más amplias, relacionadas con los deberes de colaboración e información mutua, la adaptabilidad de los recursos a las necesidades del cliente y la necesidad de la devolución útil y segura de los datos migrados, así como otras obligaciones específicas que pueden incluirse en las políticas de uso adecuado (PUA) y en el acuerdo de nivel de servicio (a modo de mínimos que materialicen el abstracto deber de diligencia del proveedor). Por último, otra diferencia radicaría en la prestación bajo demanda y en el pago por recursos consumidos que suelen ser característicos de la computación en la nube, en contraposición a las capacidades y precio predeterminados en los contratos de *Hosting*.

Como conclusión, aunque pueden compartir ciertas características y algunas obligaciones de las partes, y en algunos contratos la distinción no parece sencilla, no puede asimilarse el contrato de computación en la nube al contrato de *Hosting.* El *Cloud Computing* abarca prestaciones heterogéneas que quedan fuera del ámbito del *Hosting* (por ejemplo, softwares como servicio que ofrezcan funcionalidades que vayan más allá del mero alojamiento, o plataformas de desarrollo informático), una mayor interacción del cliente con el servicio prestado (y por tanto, una mayor asunción de responsabilidades en cuanto a contenidos y uso del servicio) y la necesidad de un deber de colaboración entre las partes más estrecho, además de otras diferencias en la remuneración del servicio. Ello no obsta para que puedan efectuarse analogías entre el concepto del contrato de *Hosting* y aquel contrato *cloud* cuyo objeto principal sea el alojamiento remoto de datos, a modo de criterio interpretativo.

3.3.- El contrato de suministro

En la prestación de los servicios de computación en la nube podemos encontrar similitudes con algunos contratos de suministro. Por ejemplo, en el contrato de suministro de energía eléctrica, puesto que ambos permiten el acceso, a través de una red, a recursos intangibles de manera continuada en el tiempo[47].

47 Otros autores han observado también que el acceso a los recursos de computación y el modo de comercialización de estos recursos a través de servicios de computación en la nube se asemeja al suministro de otros bienes, como la energía eléctrica o el gas. MARTÍNEZ MARTÍNEZ, Ricard, "El Derecho y el *Cloud Computing*", en *Derecho y Cloud Computing* (Coord. Ricard Martínez Martínez), 1ª edición, 2012, Navarra, págs. 20, 37.

Comparten también la falta de negociación entre proveedor y cliente, la adhesión de este último a condiciones generales predispuestas por el primero y el pago por uso de recursos "consumidos" (aunque recordemos que, en la computación en la nube, pueden configurarse otros mecanismos para determinar la retribución)[48]. No obstante, los recursos facilitados mediante *Cloud Computing* no siempre se "consumen" en un sentido literal, sino que en ocasiones se cede su uso al cliente, como sucede con la capacidad de almacenamiento o con el uso de funcionalidades del software que el proveedor pone a disposición del cliente. Una vez terminado el contrato, el proveedor volverá a tener disponibles los recursos que en su momento cedió (capacidad de almacenamiento, máquinas virtuales, etc.) y estos recursos podrán ser nuevamente objeto de contratos con otros clientes.

Dicho lo anterior, el contrato de computación en la nube entre empresarios debe enmarcarse dentro del ordenamiento jurídico privado. El contrato de suministro mercantil, aun siendo ampliamente utilizado en la práctica, no aparece regulado actualmente por el derecho privado[49].

La jurisprudencia, con el fin de suplir esta carencia, ha definido el suministro mercantil como "*un negocio por el que una de las partes se obliga a cambio de un precio a realizar, en favor de otra, prestaciones periódicas o continuas, cuya función es la satisfacción de necesidades continuas para atender al interés duradero del acreedor*[50]".

48 Ver apartado "Obligaciones del suscriptor: pago del precio", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

49 El legislador es consciente de la necesidad de regular esta categoría contractual, y así lo refleja en el Anteproyecto de Código Mercantil, en el cual se recoge el contrato de suministro mercantil como un tipo de contrato de intercambio de bienes, y aparece definido como aquel en el que "*el suministrador se obligará a realizar a favor del suministrado prestaciones periódicas o continuadas de los bienes objeto del contrato y aquél a pagar el precio*". Sin embargo, cabe destacar que este artículo está pensado para el suministro de "bienes muebles", con lo cual es discutible que se pueda dar cabida como tales a las capacidades informáticas que son objeto de la prestación de *Cloud Computing*. Ver, al respecto del suministro mercantil, MAROÑO GARGALLO, María del Mar; GARCÍA VIDAL, Ángel; "El contrato de suministro en el anteproyecto de Código Mercantil", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*. Getafe, Universidad Carlos III de Madrid, 2015, pp. 1373-1387. [En línea]. <http://hdl.handle.net/10016/21016>. [Fecha de consulta: 1 de marzo de 2016].

50 La Sentencia del Tribunal Supremo de 8 de julio de 1988 [RJ 1988\5589] aporta la mencionada definición. Para determinar sus reglas aplicables, primeramente deberemos acudir a lo pactado contractualmente por las partes, de acuerdo con el principio de la autonomía de la voluntad (art. 1255 del Código Civil) y subsidiariamente, al contrato de compraventa (civil o mercantil según el caso), por considerarlo la jurisprudencia de aplicación analógica, y a la teoría general de la

En nuestra opinión, son evidentes las similitudes anteriormente mencionadas[51], en especial las características esenciales del suministro mercantil, que son la continuidad y la periodicidad de las prestaciones, con el fin de atender al interés duradero o continuado del suministrado[52]. Sin embargo, aunque ambos contratos pueden considerarse de tracto sucesivo, es igualmente cierto que el contrato de suministro mercantil no refleja el conjunto de obligaciones principales que son comunes a los servicios de computación en la nube. Nos basamos, para realizar esta afirmación, en varias consideraciones.

Las primeras consideraciones que cabe mencionar hacen referencia a la concepción doctrinal de que, en el contrato de suministro, el proveedor se obliga a entregar a un cliente determinadas cosas muebles genéricas[53]. Respecto de lo anterior, el suministro de capacidades informáticas implicaría dilatar el concepto de "cosa" para que encajase en la definición tradicional del suministro[54]. Por ello, en

---

contratación (Sentencia del Tribunal Supremo, Sala de lo Civil, núm. 91/2002, de 7 de febrero). En el caso de la contratación de *Cloud Computing*, debe quedar claro que no se trata de bienes muebles, sino de servicios, con lo cual no aplicaríamos subsidiariamente la normativa sobre compraventa de los códigos Civil y de Comercio, sino la normativa sobre el arrendamiento de servicios. Opinamos que la calificación de la computación en la nube como un contrato de servicios diferenciado de la compraventa se basa en que no se adquiere, con el *Cloud Computing*, un programa informático o una herramienta, sino que se cede el uso de equipos remotos y soluciones software que pertenecen al proveedor, a través de la Red y de manera continuada en el tiempo, con lo cual el proveedor tiene otras obligaciones (deber de custodia, provisión de conectividad externa, etc.) que superan el ámbito de una mera compraventa o suministro continuado de productos informáticos o de software digital.

51 Especialmente en aquellos servicios *cloud* que no impliquen la transmisión de datos del cliente a los sistemas del proveedor, como por ejemplo, la contratación aislada de servicios de infraestructura (IaaS) de redes virtuales.

52 BERCOVITZ ÁLVAREZ, Raúl: "El contrato de suministro", *Contratos Mercantiles,* Vol. I. (Coord. Mª Ángeles Calzada; Dir. Alberto Bercovitz,), 6ª edición, Navarra, 2017, págs. 533, 534.

53 BERCOVITZ ÁLVAREZ, Raúl: "El contrato de suministro"..., *op. cit.*, págs. 530, 532.

54 El propio Código Civil ya superó la identificación entre cosa y objeto material, como ponen de manifiesto los artículos 334.10 (enumerando como bienes inmuebles las concesiones administrativas de obras públicas, servidumbres, derechos reales, etc.) y 336 (considerando las rentas o pensiones como bienes muebles). Igualmente, la doctrina mayoritaria ha superado el requisito de la corporeidad como esencial de bienes o cosas. SÁNCHEZ ROMÁN define cosa en cuanto objeto del derecho como "todo lo que es susceptible de ser sometido al poder de las personas, como medio para un fin jurídico; cuantas existencias son materia apta para la realización del derecho, en el referido concepto de medio", y distinguiendo entre cosas corporales ("cosas propiamente tales") y cosas jurídicas ("hechos o servicios productivos de utilidad")". CASTAN TOBEÑAS, la definió como "toda entidad, material o inmaterial, que tenga una existencia autónoma y pueda ser sometida al poder de las personas como medio para satisfacerles una utilidad, generalmente económica". SÁNCHEZ ROMÁN, Felipe, *Estudios de Derecho Civil,* Vol. I, 2ª edición, Madrid, 1899, pág. 43. CASTÁN TOBEÑAS, José*, Derecho civil*

cuanto a la exigencia de que los bienes objeto del suministro mercantil sean de naturaleza corporal, cabe decir que en el caso de la computación en la nube no hablaremos de bienes, sino de recursos o capacidades de computación, incorpóreas y no susceptibles de su apropiación por el cliente. Mediante el contrato se permite al cliente acceder a ellas y utilizarlas de manera temporal[55].

En cuanto al concepto de "entrega" entendido en el entorno de la computación en la nube, estas capacidades son puestas a disposición por el proveedor a través de una plataforma en la red, con lo cual no se están entregando capacidades, sino que se están poniendo a disposición del cliente para que sea este quien, cuando las necesite, pueda acceder a ellas y utilizarlas. En la nube pública, esta puesta a disposición no tiene lugar únicamente para ese concreto cliente sino para multitud de usuarios, a diferencia del contrato de suministro mercantil, que suele revestir un carácter más personalizado. Respecto de esta primera consideración, cabe decir que la Unión Europea está trabajando en la Propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales incluye como contenidos digitales datos en formato digital (vídeos, audio, aplicaciones, juegos digitales, software, etc.), y aquellos servicios que permiten la creación, el almacenamiento o la compartición de estos datos (art. 2.1), para posteriormente definir el suministro de contenidos digitales como "hecho de facilitar el acceso a contenidos digitales o poner a disposición los contenidos digitales" (art. 2.10). Según lo anterior, consideramos que la propuesta de Directiva da un nuevo sentido tanto al bien objeto del suministro como al propio concepto de suministro, diferenciándose de la tradicional noción del suministro mercantil[56].

---

español, común y foral, 15ª edición, Madrid, pág. 571. La doctrina también entiende por cosa, aunque no sea corpórea, la electricidad, y por tanto, se ha entendido el suministro eléctrico como contrato de arrendamiento de servicios y no como compraventa. SÁNCHEZ HERNÁNDEZ, Ángel, "El contrato de suministro de energía eléctrica", *Boletín de la Facultad de Derecho de la UNED*, núm. 10-11, 1996, págs. 166, 177.

55 BERCOVITZ ÁLVAREZ, Raúl: "El contrato de suministro"..., *op. cit.*, pág. 526.

56 Para más información sobre la Propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales, ver DE MIGUEL ASENSIO, Pedro, *Propuestas de Directiva sobre contratos de suministro de contenidos digitales y compraventa en línea* [en línea], 2016. Disponible en: <http://pedrodemiguelasensio.blogspot.com.es/2016/01/propuestas-de-directiva-sobre-contratos.html>. [Fecha de consulta: 11 de abril de 2017]; CASTILLO, José A., "La previsible evolución de la regulación de los contenidos digitales en el Derecho de la Unión Europea (Propuesta de Directiva 634/2015, de 9 de diciembre, sobre ciertos aspectos relativos al suministro de contenidos digitales)", *Revista Lex Mercatoria*, núm. 2, 2016, págs. 12-16; CÁMARA

La segunda consideración que permite diferenciar el suministro mercantil de la computación en la nube es la postura más activa que ocupa el cliente en relación al servicio, puesto que no aparece como un mero receptor de recursos informáticos. Dependiendo del servicio, el cliente puede gestionar la prestación en mayor o menor grado, conjuntamente con el prestador, con lo cual deberán delimitarse las responsabilidades específicas de cada uno de ellos[57].

Otra facultad que dependerá del servicio *cloud* contratado es aquella que permite al cliente procesar y almacenar en los sistemas del proveedor datos digitales que están en su haber, ya sean personales (pertenecientes a sus clientes o empleados), o datos que forman parte de su actividad empresarial: de todos ellos se espera del proveedor un deber de custodia en relación a su disponibilidad, integridad y confidencialidad. Deber que, por otro lado, es inexistente en el contrato de suministro tradicional.

Por tanto, vistas las similitudes y diferencias entre los contratos de computación en la nube y el suministro tradicional mercantil, nos decantamos por no asimilar ambas figuras jurídicas[58].

LAPUENTE, Sergio, *El régimen de la falta de conformidad en el contrato de suministro de contenidos digitales según la Propuesta de Directiva de 9 del 12 de 2015* [en línea], 2016. Disponible en: <http://www.indret.com/ca/?a=14>. [Fecha de consulta: 11 de abril de 2017]; SPINDLER, GERALD, *Contratos de suministro de contenidos digitales: ámbito de aplicación y visión general de la Propuesta de Directiva de 9.12.2015* [en línea], 2016. Disponible en: <http://www.indret.com/pdf/1243.pdf>. [Fecha de consulta: 11 de abril de 2017]; y ROSSELLÓ RUBERT, Fca. Mª., "Las contraprestaciones no dinerarias en la Propuesta de Directiva sobre suministro de contenidos digitales", *Revista de Derecho Mercantil*, núm. 303, 2017, págs. 163-190.

57 Por ejemplo, en servicios de infraestructura, el cliente puede, en ocasiones, establecer sus propias medidas de seguridad sobre la máquina virtual, mientras que el prestador se encargará de la correspondiente seguridad de los equipos informáticos hardware). Ver "Figura 2: modelo de servicios en la computación en la nube", en el capítulo "Concepto y características técnicas de la computación en la nube", y capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

58 En la descartada Propuesta de Normativa Común de Compraventa Europea (COM 2011 635 final), en su considerando 17 bis, se identificó suministro de contenidos digitales y computación en la nube: "La computación en nube se está desarrollando a gran velocidad y tiene un gran potencial de crecimiento. La normativa común de compraventa europea prevé un conjunto coherente de normas adaptadas al suministro a distancia, y en particular al suministro en línea, de contenidos digitales y servicios relacionados. Debe ser posible que esas normas también se apliquen cuando el contenido digital o los servicios relacionados se suministren utilizando una nube, en particular cuando el contenido digital se pueda descargar desde la nube del vendedor o almacenarse temporalmente en la nube del prestador de servicios". Por lo anteriormente analizado, no creemos acertada esta asimilación de conceptos, que si bien puede resultar útil para explicar *a grosso* modo el funcionamiento de la nube y de la Web 2.0 (es

3.4.- El contrato de depósito

Al igual que sucede con el suministro, existen ciertas similitudes entre los contratos de computación en la nube y el contrato de depósito que pueden plantear la posible coincidencia de su naturaleza jurídica. En principio, cabe destacar que estas coincidencias únicamente pueden predicarse de aquellos contratos *cloud* que impliquen la migración de datos del cliente al proveedor[59], al implicar ambos un servicio de guarda y custodia[60]. Así, consideramos que aquellos contratos que permitan el alojamiento remoto de información presentan caracteres compartidos con el depósito del art. 1758 del Código Civil, dado que, de acuerdo con el precepto mencionado, "[el depósito] se constituye desde que uno recibe la cosa ajena con la obligación de guardarla y de restituirla", puesto que la conservación y guarda y custodia de lo depositado, así como su restitución, aparecen como obligaciones básicas de todo depósito[61]. Igualmente, en el contrato de computación en la nube entre empresarios se dan condiciones concordantes con el art. 303 del Código de Comercio, con lo cual podría aplicarse

---

decir, el acceso a través de Internet a capacidades informáticas, entre ellas contenidos digitales: software, vídeos, archivos, bases de datos, etc.), no se corresponde con las características del contrato atípico y complejo de *Cloud Computing*. La misma asimilación de conceptos tiene lugar en su relevo, la actual Propuesta de Directiva del parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales (COM (2015) 634 final). La Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales, engloba el software como servicio en sentido amplio (aplicaciones, juegos, vídeos, almacenamiento, etc.) y regula las obligaciones del proveedor con el consumidor de estos servicios. En todo caso, utilizaremos en todo este trabajo un concepto deliberadamente amplio de "suministro", cercano al recogido por la Propuesta de Directiva sobre suministro de contenidos digitales.

59 Un ejemplo de contrato *cloud* que no implica la migración de datos a servidores del proveedor puede ser aquel que tenga por objeto la implementación de una red virtual o la utilización de un software que no implique el almacenamiento de contenidos. Sin embargo, es poco frecuente que este tipo de servicios se contraten aisladamente, sino que suelen formar parte de un paquete de servicios de infraestructura o plataforma.

60 "[En el depósito civil], la obligación de guarda y custodia no se traduce en una obligación más en el sinalagma contractual, sino que es la principal de quien la posee, y a la vez, causa y esencia del contrato". ÁLVAREZ LATA, Natalia [et al.]; "Contratos de prestación de servicios y realización de obras. 2.- Servicios de guarda y custodia", *Tratado de contratos*, (Dir. Rodrigo Bercovitz) 1ª edición, Valencia, 2009, pág. 2913. Según el Tribunal Supremo, el carácter esencial de esta obligación permite distinguirla de otras modalidades contractuales, generalmente atípicas, como el contrato de exposición de obra de arte (STS de 22 de enero de 2002).

61 Art. 1758 del Código Civil: "Se constituye el depósito desde que uno recibe la cosa ajena con la obligación de guardarla y de restituirla". Hablamos, en todo caso, de depósito voluntario (art. 1763 y ss del Código Civil).

analógicamente la normativa relativa al depósito mercantil[62], y las disposiciones civiles con carácter supletorio. En este aspecto, también resulta interesante, debido a la semejanza de la obligación de guarda y custodia, la eventual aplicación analógica de algunas de las disposiciones del depósito civil, en cuanto a la retención o el uso sin autorización de los datos del cliente por parte del proveedor *cloud*, cuando en los contratos predispuestos no se reconozca la obligación de la disponibilidad y la restitución de los datos al cliente como obligación principal del proveedor de servicios de computación en la nube[63].

Como se ha dicho, los servicios *cloud* que suponen migración de datos del cliente y el depósito coinciden, pues, en la obligación de guardar lo depositado con la diligencia exigible conforme a la *lex artis*, cuando se trate de depósito mercantil[64], y restituirlo cuando lo exija el cliente, como objeto esencial del acuerdo[65]. Aun así, tras

62 Art. 303 del Código de Comercio: "Para que el depósito sea mercantil se requiere:1º.- Que el depositario, al menos, sea comerciante. 2º.- Que las cosas depositadas sean objeto de comercio. 3º.- Que el depósito constituya por sí una operación mercantil, o se haga como causa o a consecuencia de operaciones mercantiles".

63 Ver ROSSELLÓ RUBERT, Francisca Mª, "La recuperación de los contenidos alojados y su portabilidad; en especial, su previsión por el Reglamento 2016/679 General de Protección de Datos de la UE", *Hacia una justicia 2.0, Actas del XX Congreso Iberoamericano de Derecho e Informática* (Dir. Federico Bueno de Mata), Salamanca, 2016, págs. 283 a 298. Asimismo, ver "El derecho a la recuperación de los datos y a la portabilidad" en el capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

64 La *lex artis* se exige a entidades depositarias profesionales, y se considera bastante más estricta que el deber de diligencia genérico "del buen padre de familia", fundamentado en la habitualidad con la cual realiza la prestación de este tipo de servicios, el ánimo de lucro y la exteriorización de esa actividad económica. Ver, respecto de la *lex artis* en relación con el depósito, OZCÁRIZ MARCO, Florencio, *El contrato de depósito. Estudio de la obligación de guarda,* 1ª edición, Barcelona, 1996, pág. 292-295. En relación al depósito de mercancías prestado por una entidad profesional, se ha calificado el deber de conservación de lo depositado como una obligación de medios, y a nuestro parecer, lo anterior resulta aplicable analógicamente a los contratos *cloud* que impliquen la migración de datos del cliente, en los que la entidad depositaria profesional deberá utilizar todos los medios que tenga a su disposición para conservar lo depositado y evitar su menoscabo ("Así, el deber de conservación, guarda y custodia se ve investido de un marcado carácter técnico y cualificado en el más alto nivel, que hace que el deber vaya más allá de la mera vigilancia de la mercancía depositada y comprenda todas las acciones necesarias y convenientes para su control, protección y su mantenimiento, inalterada e incólume y apta para los fines que le fueron atribuidos inicialmente (...)") Este compromiso no alcanza, en la computación en la nube, la garantía absoluta en relación a la seguridad integral de los datos, y, por tanto, no es susceptible de considerarse una obligación de resultado. MARCO ALCALÁ, Luis Alberto; "Contratos de Depósito y Contratos Análogos", Contratos Mercantiles Vol. I. (Coord. Mª Ángeles Calzada; Dir. Alberto Bercovitz), 3ª edición, Navarra, 2007, pág. 729. Ver capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

65 MARCO ALCALÁ, Luis Alberto; "Contratos de Depósito...", *op. cit.*, pág. 728.

esta inicial similitud entre ambas figuras, resulta conveniente realizar algunos matices.

El primero de ellos, en cuanto a la naturaleza de aquello que el proveedor de computación en la nube está obligado a custodiar, puesto que no son bienes muebles, objeto del contrato clásico de depósito, sino información digital intangible[66]. A veces, los contenidos alojados en la nube serán ejemplares originales y "únicos", puesto que el cliente de servicios *cloud* puede carecer de una copia de los contenidos en sus sistemas, o disponer en la nube de contenidos editados, modificados o no totalmente coincidentes con los que almacena en su equipo, con lo cual al cliente le interesará recuperar aquellos contenidos migrados. En otras ocasiones, la migración implicará copias de contenidos digitales que el cliente habrá alojado en la nube a modo de copia de seguridad o para poder realizar otras funciones que el servicio *cloud* le permita (compartir esos contenidos con otros usuarios, procesarlos, poder acceder a ellos a través de diferentes dispositivos a través de la red, etc.), con lo cual en su uso del servicio no habrá implicado realmente una transmisión de la posesión de esos contenidos originales, sino la transmisión de una copia[67]. El proveedor *cloud*, por su parte, generalmente efectuará replicados en sus sistemas y dispondrá de un plan de recuperación del servicio en caso de producirse problemas de seguridad (*disaster recovery plan*), como parte de su deber de diligencia profesional[68].

El segundo matiz va referido al conjunto de obligaciones para ambas partes que implica el servicio de computación en la nube, en relación al contrato de depósito, puesto que el deber de custodia no supone la única finalidad esencial del contrato, sino que es una de las obligaciones que asume el proveedor al habilitar el almacenamiento remoto de datos del cliente. Además, la computación en la nube

66 Art. 1761 del Código Civil: "*Sólo pueden ser objeto del depósito las cosas muebles*". Ello es así porque el tipo "*precisa específicamente la entrega al depositario, esto es, el desplazamiento posesorio*", lo cual "*lleva a exigir también (...) la corporeidad de la cosa"* y a predicar la naturaleza real del contrato de depósito civil. ÁLVAREZ LATA, Natalia [et al.]; "Contratos de prestación de servicios y realización de obras...", *op. cit.*, pág. 2914 y ss.

67 YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet..., op. cit.,* pág. 329, en relación a la distinción entre el contrato de *Hosting* y el contrato de depósito.

68 Por ello, en nuestra opinión, es independiente el uso que el cliente realice del servicio, sea para almacenar contenidos únicos o copias, puesto que persiste en el proveedor la obligación de mantener su conservación y custodia, y facilitar al cliente la recuperación de estos contenidos. Ver apartado "Obligaciones del proveedor: la adopción de una política de seguridad adecuada", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

puede implicar otras capacidades informáticas (potencia de procesamiento, capacidad de red, etc.) distintas a la capacidad de almacenamiento, y otros servicios igualmente esenciales que debe prestar el proveedor (conectividad externa, etc.). Entre estos deberes, destaca la verdadera razón de la contraprestación del cliente *cloud:* el acceso ininterrumpido y remoto a los recursos que le facilita el proveedor, que generalmente no se reducen al almacenamiento de datos, sino que se extienden a las funcionalidades de la interfaz y de demás software que acompaña a tales recursos. Combinadas, ambas herramientas (capacidad informática y software de autogestión) permiten al cliente abastecerse de recursos de computación de acuerdo con sus necesidades, pudiendo ser una de ellas, pero no la única, la funcionalidad que permite almacenar remotamente datos digitales.

Otra diferencia radica en la propia prestación del servicio *cloud,* caracterizado por ser de tracto sucesivo. Como se ha observado anteriormente, forma parte de la prestación permitir al cliente *cloud* el acceso y procesado de los datos migrados mientras subsista la relación jurídica, aunque no estará recuperándolos definitivamente, sino que este acceso tiene lugar de forma remota y mientras el proveedor continúa custodiándolos en sus sistemas. Como vemos, este acceso remoto a partir de cualquier dispositivo con conexión a Internet forma parte de la propia prestación de los servicios en la nube, con lo cual no implica el fin de la relación jurídica por restitución de lo depositado, como sucede con el depósito. Ello no obsta para que, como hemos apuntado, una vez extinguida la relación contractual con el proveedor *cloud*, los datos (o una copia de estos) deban ser puestos a disposición del cliente de manera que pueda recuperarlos con el fin de seguir utilizándolos en sus propios sistemas o en los de otro proveedor, y posteriormente sean eliminados de los sistemas del proveedor una vez extinguida la relación contractual. Obligación, por otra parte y a nuestro parecer, semejante al deber de restitución, considerado como esencial en el contrato de depósito.

Dicho lo anterior, podemos concluir que las obligaciones principales del contrato *cloud* no se reducen al almacenamiento de datos del cliente y a proceder a su devolución, sino que implican otros deberes para ambas partes que no encajan con la figura del depósito, con lo cual uno y otro contrato no pueden considerarse equivalentes en términos jurídicos.

3.5.- El contrato de licencia de uso no personalizada de software

Se entiende por licencia de uso no personalizada de un programa de ordenador "aquel contrato por medio del cual el titular de los derechos de explotación de un programa de ordenador transfiere los derechos de reproducción necesarios para la utilización de una copia del mismo a un tercero, usuario final, que viene determinado en cada caso por la legítima posesión de dicha copia, al tiempo que regula las principales circunstancias del uso lícito del programa, singularmente el régimen de responsabilidad al que se somete el licenciante ante la existencia de vicios o errores en el software adquirido"[69]. Esta licencia faculta al usuario (final e indeterminado) del software a aprovechar sus características técnicas, y a integrarlo dentro de su operativa empresarial en aquellos casos en los que el licenciatario sea un empresario o profesional, pero no a obtener lucro mediante su explotación o la venta de copias de ese programa[70].

Las licencias de uso no personalizadas de software (pensadas para programas informáticos distribuidos en masa) tienen como objeto "las cláusulas relativas a la reproducción del programa (generalmente, número de copias permitidas, almacenaje, ejecución simultánea o en red y otras del estilo)"[71], y alcanzan el propio programa informático, los soportes materiales en los cuales se plasma, y los manuales y documentación electrónica que acompañan a estos soportes[72].

Los contratos de computación en la nube fácilmente pueden confundirse con contratos de licencia de uso de software, puesto que parte de la relación jurídica entre el proveedor *cloud* y su cliente consiste en permitir el uso al cliente de un programa de ordenador, entre otras prestaciones. Ello es así independientemente de la capacidad objeto del contrato *cloud*, puesto que, al tratarse de capacidades informáticas distribuidas a través de Internet y a modo de autoservicio, siempre se verán implicados programas informáticos de diversa índole (sistemas operativos o programas de base que permiten al usuario administrar la máquina virtual o la capacidad proporcionada por el servicio de infraestructura; herramientas software de diseño, desarrollo y ejecución de programación informática de los servicios de plataforma; o funcionalidades de las aplicaciones proporcionadas a modo de software como servicio)[73]. Así, como vemos, la licencia de uso de programa informático no

69 APARICIO VAQUERO, Juan Pablo; *Licencias de uso ..., op. cit.,* pág 78.
70 APARICIO VAQUERO, Juan Pablo; *Licencias de uso ..., op. cit.,* pág 79 y ss.
71 APARICIO VAQUERO, Juan Pablo; *Licencias de uso ..., op. cit.,* pág 16.
72 APARICIO VAQUERO, Juan Pablo; *Licencias de uso ..., op. cit.,* pág 16.
73 En cuanto a los tipos de software involucrados en la computación en la nube, ver capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

solo está estrechamente relacionada con el contrato de computación en la nube, sino que el contrato de servicio *cloud* incluirá cláusulas relativas a la licencia de uso del software, con la finalidad única de facultar y regular el acceso del cliente a los servicios facilitados por el proveedor *cloud* (entre ellos la utilización del software implicado en la prestación del servicio) para que el cliente pueda utilizarlos y disfrutar de una prestación eficiente.

Por tanto, consideramos que no se puede sostener la coincidencia entre ambos contratos, los dos atípicos, puesto que la licencia será parte integrante del contrato de computación en la nube, sea cual sea la capacidad contratada[74]. La licencia de uso no personalizada contiene, por una parte, aspectos referentes a la propiedad intelectual y, por otra, aspectos relativos a la delimitación de responsabilidades entre titular del programa y destinatario.

En el contrato de computación en la nube se recogen generalmente una serie de cláusulas dedicadas a la licencia de uso del software, en las que se regulan aspectos relacionados con la propiedad intelectual sobre el software que el proveedor *cloud* pone a disposición del cliente a través del servicio (permiso para utilizar y/o descargar el software en uno o múltiples equipos, posibilidad del uso concurrente por diferentes usuarios, prohibición de ingeniería inversa y copia ilegal, estipulaciones relacionadas con el uso de logotipos y marcas registradas, posibilidad o no de crear nuevas versiones del software o aplicaciones relacionadas.

Los contenidos relativos a la licencia de uso, y concretamente, las limitaciones y prohibiciones relacionadas con el uso del programa por parte del cliente *cloud* suelen recogerse dentro de las llamadas políticas de uso adecuado del servicio (PUA), junto con el resto de restricciones del uso del servicio que deban observar los usuarios de los servicios de *Cloud Computing*. Mientras, la distribución de las responsabilidades entre el cliente y el proveedor del servicio derivadas de errores del software o de su mal uso se englobarán generalmente en apartados dedicado a las

74 Afirma APARICIO VAQUERO que la atipicidad de la licencia de uso radica en la causa del objeto (permitir el uso de un programa informático) y su alcance (restringido al mero uso en las condiciones pactadas y no a la explotación económica del software), distinguiéndose del contrato de explotación de obra intelectual de los arts. 43 y ss de la Ley de Propiedad Intelectual, APARICIO VAQUERO, Juan Pablo; *Licencias de uso ..., op. cit.,* pág 293. TERRADO SÁNCHEZ, por su parte, lo califica como arrendamiento de servicios. TERRADO SÁNCHEZ, Federico, "La diversidad contractual en la generación y explotación de bases de datos", *Informática y Derecho: Revista Iberoamericana de Derecho Informático,* núm. 9-10-11, Vol. 1, 1996, págs. 301-317.

responsabilidades de las partes, donde se recogerán no solo aquellas obligaciones de responder por problemas derivados del software cedido, sino cualquier otra cuestión sobre incidencias relacionadas con el funcionamiento global del servicio *cloud*. En capítulos posteriores abordaremos el estudio de las cuestiones relacionadas con la cesión de uso de software, las políticas de uso adecuado y las obligaciones y responsabilidades de las partes del contrato de computación en la nube.

La licencia de uso de software, aun formando parte del contrato de computación en la nube, no alcanza a regular muchas de las obligaciones de las partes del contrato de computación en la nube. En especial, el papel del proveedor *cloud* es más activo que el de un mero cedente de derechos de uso, puesto que debe garantizar la continuidad de la prestación mediante la conectividad externa y la actualización y mantenimiento constantes del entorno, debe implementar medidas de seguridad para proteger la información migrada, etc. El cliente, por su parte, tiene una relación más estrecha con el proveedor *cloud* que supera el vínculo entre licenciante y licenciatario, derivado, sobre todo, del diseño como autoservicio de la prestación (y, por tanto, de su posibilidad de configurar en mayor o menor medida ciertos aspectos de ese servicio) y de la interrelación con la capacidad objeto del contrato, especialmente, cuando el servicio permite el almacenamiento de datos del cliente en sistemas remotos controlados por el proveedor.

Para finalizar con esta comparativa, podemos decir que no cabe, a nuestro modo de ver, la identificación entre los contratos de licencia de uso no personalizada de software y el contrato de computación en la nube, aunque están relacionados, puesto que como parte integrante del contrato de computación en la nube generalmente encontraremos licencias que restringirán al suscriptor el uso de software implicado en la prestación del servicio.

Como conclusión a este apartado, podemos afirmar que, si bien el contrato de computación en la nube comparte características comunes con otras figuras jurídicas y contratos habituales del tráfico mercantil, no puede identificarse plenamente con ninguno de ellos, debiendo calificarse, como veremos en el apartado siguiente, como contrato atípico reconduciéndose su regulación al genérico contrato de servicios.

4.- NATURALEZA JURÍDICA DE LOS CONTRATOS DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

Tras la exposición, en apartados anteriores de este capítulo, de la pluralidad de potenciales prestaciones que pueden ser objeto de la contratación de servicios de computación en la nube, y teniendo en cuenta la diversidad de modalidades de implementación de la computación en la nube, podemos deducir que la determinación de la naturaleza jurídica de este tipo de contratación resulta una cuestión compleja aunque necesaria, puesto que nos permitirá establecer qué criterios jurídicos interpretativos pueden aplicarse para solucionar eventuales conflictos[75].

A continuación, trataremos las características comunes de la contratación de los diferentes servicios de computación en la nube pública, para posteriormente determinar su naturaleza jurídica. Por último, finalizaremos el capítulo que nos ocupa con una aproximación al concepto de contrato de computación en la nube pública.

4.1. Características de los contratos de servicios de computación en la nube

En este apartado, nos detendremos en las características comunes que presentan los contratos *cloud* bajo la modalidad de implementación de nube pública, centrándonos principalmente en aquellos suscritos por pequeños empresarios que, como hemos mencionado, forman el objeto de estudio de este trabajo.

4.1.1.-Contrato mercantil

Aunque este trabajo se centra en la contratación interempresarial, lo cierto es que, a diferencia de otros supuestos (como sucede con el *Outsourcing*[76]), no es esta

75 Como hemos visto en el capítulo "Concepto y características técnicas de la computación en la nube", existen cuatro modalidades de implementación: nube privada, nube comunitaria, nube pública y nube híbrida. Como hemos puntualizado en anteriores ocasiones, nuestro trabajo acota el ámbito de la contratación *cloud* a la modalidad de implementación pública y, más concretamente a los contratos de adhesión susceptibles de ser suscritos por el pequeño empresario.

76 En consideración de APARICIO VAQUERO, en el *Outsourcing* informático ambas partes contractuales tienen la categoría de empresarios, y, al ser una técnica de gestión empresarial consistente en la externalización de la actividad informática de una empresa, "no cabe hablar de

una de sus características esenciales, sino que, de hecho, muchos servicios de computación en la nube pública son ampliamente suscritos por consumidores, especialmente la categoría del software como servicio (SaaS). En tales casos, el contrato tendrá naturaleza civil y será aplicable la normativa sobre protección de consumidores.

En cuanto a los contratos en los que centramos esta tesis, es decir, aquellos suscritos por pequeños empresarios, desde la perspectiva de las partes de la relación jurídica puede afirmarse que estos contratos tienen carácter mercantil, puesto que la prestación del servicio constituye la actividad económica del proveedor, y se integrará en la actividad empresarial, comercial o profesional del cliente[77]. Sin embargo, como veremos, debemos reconducir su regulación, de momento, a disposiciones de otros contratos típicamente civiles (como el contrato de arrendamiento de servicios), a la espera de que puedan regularse en un futuro los contratos de computación en la nube u otras nuevas figuras jurídicas mercantiles que puedan resultarnos más próximas, como la prestación de servicios mercantiles en general, la licencia de bienes inmateriales, el alojamiento remoto de datos o el suministro mercantil, todas ellas figuras carentes de regulación en nuestro Código de Comercio actual, aunque previstas en el Anteproyecto de Código Mercantil[78].

4.1.2.- Contrato consensual

El contrato de computación en la nube se forma a través del acuerdo entre las partes, de manera consensual (arts. 1254 y 1258 del Código Civil[79]) y, especialmente aquellos contratos suscritos por consumidores y pequeños empresarios, tiene lugar en sede electrónica. La Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en su anexo, define el "contrato

---

contratos de Outsourcing entre consumidores". APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática..., op. cit.*, págs. 33 y 82.

77 La misma consideración se ha realizado del *Outsourcing*. APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática..., op. cit.*, págs. 82-83.

78 A mayor abundamiento, queremos comentar que en el Anteproyecto de Código Mercantil aparece una nueva categoría de contratos: los "contratos para las comunicaciones electrónicas", entre los cuales se encuentra, como se ha visto, el "contrato de alojamiento de datos".

79 Art. 1254 del Código Civil*:* "El contrato existe desde que una o varias personas consienten en obligarse, respecto de otra u otras, a dar alguna cosa o prestar algún servicio". Art. 1258 del Código Civil: "Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan, no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley".

electrónico" o "contrato celebrado por vía electrónica" como "todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones"[80]. Internet se configura como la red de telecomunicaciones que posibilita la contratación *cloud* que nos ocupa[81], con lo cual nos encontramos ante lo que viene denominándose un contrato *online* o en línea, en el sentido en que se perfecciona a través de una página web y puede suscribirse en masa gracias a programas informáticos de contratación y condiciones generales predispuestas por el proveedor[82].

De manera excepcional, pueden existir en el mercado contratos de computación en la nube para pequeñas empresas en los que, por su implementación (privada o comunitaria), por exigencias de la personalización del servicio, o por dimensión y motivos comerciales del proveedor, ambas partes se encuentren en posición de debatir y negociar las diferentes cláusulas contractuales que integrarán un posible acuerdo futuro. Sin embargo, cuando hablamos de la modalidad pública de implementación de la nube, la regla general es la suscripción de contratos de adhesión, entendidos como "aquellos en que existe una previa prerredacción unilateral del contrato que es obra de una de las partes contratantes, por medio de formularios, impresos, pólizas o modelos preestablecidos, y a la otra sólo le es permitido declarar su aceptación o eventualmente su rechazo"[83]. En la computación en la nube, la parte que redactará las cláusulas de adhesión será el proveedor *cloud* y el cliente empresario o particular será quien las suscriba[84].

---

80 No nos detendremos, por exceder del objeto de este trabajo, en el análisis detallado de la definición de "contrato electrónico" realizada por la LSSI, sino que únicamente nos limitaremos a calificar el contrato de computación en la nube como contrato electrónico, de acuerdo con la literalidad del artículo. Para una explicación más detallada, nos remitimos a MENÉNDEZ MATO, Juan Carlos, *El contrato vía Internet,* 1ª edición, Barcelona, 2005, pág. 162.

81 Por su parte, la doctrina ha caracterizado a Internet como una red global abierta y sin propietario, global, que permite proporcionar servicios interactivos y concluir contratos e incluso ejecutarlos íntegramente, en ciertos supuestos. MENÉNDEZ MATO, Juan Carlos, *op. cit.*, pág. 41.

82 Se excluyen, mediante esta acepción, contratos concluidos entre dos sujetos directamente, sirviéndose para ello del uso de correo electrónico, videoconferencia o *chat*, que sí se consideran, por otra parte, contratos electrónicos. MENÉNDEZ MATO, Juan Carlos, *op. cit.*, pág. 169.

83 DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. I. Introducción. Teoría del contrato*, 6ª Edición, Navarra, 2007, pág. 166.

84 En capítulos posteriores se realizará una propuesta de aplicación extensiva de la normativa de protección de consumidores y usuarios a aquellos pequeños empresarios que compartan la posición débil del consumidor. Ver apartado "Breve reflexión relativa a la aplicación extensiva de las normas y criterios sobre cláusulas abusivas al pequeño empresario. Extensión al ámbito de la contratación de servicios de *Cloud Computing*", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

4.1.3.- Contrato bilateral

El contrato de computación en la nube es un contrato bilateral y sinalagmático entre el prestador de servicios y el pequeño o mediano empresario, profesional o usuario del servicio, puesto que crea obligaciones recíprocas a cargo de ambas partes, aunque estas no se encuentran en igualdad de condiciones, sino que el proveedor ostenta, generalmente, una posición dominante en la relación negocial[85].

4.1.4.- Contrato oneroso

La definición que realiza el *National Institute of Standards and Technology* (NIST) sobre la computación en la nube deja entrever que los contratos de servicios de computación en la nube se remuneran, generalmente, de acuerdo con la monitorización que realiza el proveedor del consumo de recursos del cliente, permitiendo ajustar el precio a la capacidad suscrita contractualmente y al efectivo volumen de recursos consumidos[86]. Igualmente, el proveedor puede establecer otras modalidades de tarifado, como por ejemplo una tarifa plana que permita el acceso del recurso hasta un cierto límite de su capacidad, o una retribución que atienda al número de usuarios de la empresa cliente con acceso al servicio[87]. En estos casos, nos hallaremos ante un contrato claramente oneroso, puesto que supone contraprestaciones por ambas partes, y correlativamente, ambas partes obtienen ventajas del negocio jurídico[88].

En otras ocasiones, puede suceder que el cliente empresario admita, a cambio del acceso al servicio, contraprestaciones de naturaleza no dineraria (como soportar

85 DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. I..., op. cit.*, págs 167-168.

86 Como recordaremos, la definición realizada por el NIST del *Cloud Computing* es la siguiente: "El *Cloud Computing* es un modelo para proporcionar el acceso, bajo demanda y a través de la red, a un conjunto de recursos compartidos configurables (por ejemplo: redes, servidores, almacenaje, aplicaciones y servicios) que pueden ser rápidamente suministrados y lanzados al cliente con un sencillo manejo y con mínima interacción con el proveedor. Se compone de cinco características, tres modelos de servicio y cuatro modelos de implementación". (Traducción propia). NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST; *Special Publication 800-145. The NIST definition for Cloud Computing.* [en línea], 2011. Disponible en: <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. [Fecha de consulta: 11 de abril de 2017].

87 Por ejemplo, un software como servicio de almacenamiento que permita al cliente acceder a *x Gigabytes* de memoria por un precio *y*. En cuanto a aquellos usos que excedan ese límite, la facturación puede combinarse con el consumo de recursos efectivo de recursos, por ejemplo, un devengo de *z* por cada *Gigabyte* extra consumido.

88 DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. I..., op. cit.,* pág. 99.

publicidad, que se utilice el logotipo, nombre o marca registrada del cliente para propósitos publicitarios del proveedor, o acceder a formar parte de bases de datos), con lo cual el contrato de computación en la nube no pierde su calidad de oneroso (art. 1274 del Código Civil[89]). Así sucede, por ejemplo, con algunos contratos *cloud* de software como servicio (SaaS) de correo electrónico o almacenamiento remoto. Desde nuestra perspectiva, difícilmente los contratos de computación en la nube, y especialmente aquellos destinados a pequeñas y medianas empresas, pueden ser considerados contratos gratuitos, dado que suponen contraprestaciones para ambas partes[90], aunque, debido a la naturaleza no dineraria de las contrapartidas del cliente, este pueda parecer un mero beneficiario a título gratuito de la prestación del proveedor. Sin embargo, la contraprestación del cliente tiene a menudo interés comercial para el proveedor *cloud*[91].

Por ello, la falta de contraprestación dineraria no supone en modo alguno que estas relaciones jurídicas no tengan sean vinculantes para las partes, tal y como reconocen los términos de los acuerdos cuya suscripción se requiere para que el cliente pueda acceder a la plataforma y disfrutar del servicio[92].

La Propuesta de Directiva sobre suministro de contenidos digitales reconoce

89 Art. 1274 del Código Civil: "En los contratos onerosos se entiende por causa, para cada parte contratante, la prestación o promesa de una cosa o servicio por la otra parte; en los remuneratorios, el servicio o beneficio que se remunera, y en los de pura beneficencia, la mera liberalidad del bienhechor".

90 En relación a la onerosidad y gratuidad de los contratos, tomamos como referencia a DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. I..., op. cit.,* pág. 99.

91 Muchos servicios que se ofertan en la red como gratuitos son empresas altamente rentables y son importantes valores bursátiles. Como ejemplo, la plataforma de contactos profesionales *LinkedIn*, una aplicación de red social especializada en contactos profesionales (es decir, un software como servicio) que permite abrir a sus clientes cuentas sin necesidad de contraprestación dineraria (aunque también permite cuentas *premium*) ha sido adquirida recientemente por la multinacional Microsoft por 23.260 millones de euros, y sus acciones se valoraron el día de la transacción en 193 dólares cada una. La red social *Facebook*, que se promociona como gratuita, se valoró en noviembre de 2015 por más de 281.000 millones de euros, es decir, tanto como las españolas *Telefónica, Inditex*, *Banco Santander* y *BBVA* juntos. Ver noticias en <http://economia.elpais.com/economia/2016/06/13/actualidad/1465821508_909017.html> y <http://www.elmundo.es/economia/2015/11/05/563bbf7846163fe60f8b4635.html>, respectivamente. [Fecha de consulta: 11 de abril de 2017].

92 Por ejemplo, las condiciones del software como servicio de almacenamiento *Box* asumen el acuerdo sin contraprestación dineraria como contenido contractual*:* "Le damos la bienvenida a Box. Lea atentamente estos términos y condiciones ("Condiciones) de uso de los servicios. Una vez aceptados, constituyen un contrato ("Contrato") entre usted y Box.com Ltd, (...) que regula su acceso y uso de los servicios de Box (...)*"*. Disponibles en: <https://www.box.com/legal/termsofservice/ES/>. [Fecha de consulta: 11 de abril de 2017].

la naturaleza onerosa de contratos de suministro de contenidos digitales aun cuando la contraprestación sea de carácter no pecuniario, y afirma en su considerando 13 que la aplicabilidad de esta futura norma no debe depender del precio, puesto que, en estos casos, el contenido digital no se suministra realmente de forma gratuita[93]. En su artículo 3.1, que establece el ámbito de aplicación de la norma, se advierte de la no distinción entre contratos remunerados monetariamente y contratos remunerados con datos respecto de los derechos y obligaciones recogidos en la norma: "La presente Directiva se aplicará a cualquier contrato en virtud del cual el proveedor suministra contenidos digitales al consumidor o se compromete a hacerlo y, a cambio, se paga un precio o el consumidor facilita activamente otra contraprestación no dineraria en forma de datos personales u otro tipo de datos"[94].

De este modo, como veremos más detalladamente en apartados posteriores, el *Cloud Computing* es susceptible de considerarse un contrato de servicios puesto que, aunque en ocasiones pueda aparentar ser un contrato gratuito, en la inmensa mayoría de casos el cliente está sujeto a cargas o cesiones (soportar publicidad, ceder

93 Propuesta de Directiva sobre suministro de contenidos digitales. Considerando 13: "Con frecuencia los contenidos digitales no se intercambian por un precio, sino por una contraprestación diferente al dinero, es decir, permitiendo el acceso a datos personales o a otro tipo de datos. Estos modelos de negocio específicos se aplican de diferentes formas en una parte considerable del mercado. La introducción de una diferenciación dependiendo de la naturaleza de la contraprestación generaría una discriminación entre los diferentes modelos de negocio, ofrecería un incentivo injustificado a las empresas para orientarse hacia la oferta de contenidos digitales a cambio de datos. Deben garantizarse condiciones equitativas. Además, los defectos en las características de funcionamiento de los contenidos digitales suministrados por una contraprestación diferente al dinero afectan a los intereses económicos de los consumidores. Por tanto, la aplicabilidad de las normas de la presente Directiva no debe depender del precio pagado por el contenido digital específico en cuestión".

94 Sin embargo, el mismo artículo excluye de su aplicación datos personales necesarios para la prestación del servicio o para cumplir exigencias legales, siempre que no se destinen a otras finalidades: "La presente Directiva no se aplicará a contenidos digitales suministrados por una contraprestación no dineraria en la medida en que el proveedor solicite del consumidor datos personales cuyo tratamiento sea estrictamente necesario para la ejecución del contrato o para cumplir requisitos legales, y el proveedor no los someta a otro tratamiento que sea incompatible con este fin. Tampoco se aplicará a ningún otro dato que el proveedor solicite del consumidor con el fin de garantizar que los contenidos digitales son conformes con el contrato o cumplir requisitos legales, y el proveedor no utiliza dichos datos con fines comerciales". La contraprestación no dineraria, sin embargo, sí puede servir a modo de criterio moderador e interpretativo para determinar la conformidad de los contenidos digitales con el contrato, como establece su artículo 6.2: "En el supuesto de que el contrato no establezca, cuando proceda, de forma clara y comprensible, los requisitos para los contenidos digitales de conformidad con el apartado 1, estos serán aptos para los fines a los que ordinariamente se destinen contenidos digitales del mismo tipo,(...), teniendo en cuenta: a) si los contenidos digitales se suministran a cambio de un precio o por otra contraprestación no dineraria; (...)". Para un estudio más detallado, nos remitimos a ROSSELLÓ RUBERT, Fca. M, "Las contraprestaciones no dinerarias en la Propuesta de Directiva sobre suministro de contenidos digitales", *Revista de Derecho Mercantil,* núm. 303, 2017, págs. 163 a 190.

datos personales u otra información para usos comerciales, etc.) como condiciones para el uso del servicio.

Por otra parte, la falta de contraprestación dineraria sí se presenta como un factor esencial en relación a la redacción de las cláusulas contractuales, especialmente, en cuanto a la exención contractual de responsabilidades por culpa del proveedor y a la asunción de riesgos derivados de la ejecución del contrato por parte del cliente. Si el contrato no se sujeta a contraprestación dineraria, el proveedor tiende a exonerarse al máximo de cualesquiera responsabilidades derivadas del uso del servicio. Del mismo modo, y tal como reconocen ciertos autores, los Tribunales, de acuerdo con el art. 1103 del Código Civil[95], podrán ejercer su facultad moderadora y decidir, atendiendo a la falta de contraprestación dineraria y a la naturaleza y efectos de los daños ocasionados, si existe o no la obligación de responder por parte del proveedor, y, en su caso, intervenir en la determinación de indemnizaciones a los perjudicados[96].

4.1.5 -Contrato de tracto sucesivo que se presta por medios electrónicos

Uno de los rasgos distintivos del contrato *cloud* es su configuración como contrato de tracto sucesivo, es decir, se presta de manera continuada en el tiempo, durante el cual se prolonga la relación entre el cliente y el proveedor. La configuración de la duración de este contrato de tracto sucesivo variará dependiendo del proveedor, y generalmente son vinculantes desde que se suscriben, y a partir de ese momento se originarán las eventuales contraprestaciones económicas para el cliente.

En muchos casos, los contratos no establecen un plazo de duración, sino que son de duración indefinida, permaneciendo vigentes hasta que una de las partes termine el contrato. En estos casos, los motivos de terminación se incluirán en el contrato a modo cláusulas resolutorias, enumerando las razones que permitirán extinguir la relación contractual tanto por una como por otra parte. Por ejemplo, el proveedor puede reservarse el derecho de terminar el contrato cuando el cliente

95 Art. 1103 del Código Civil: "La responsabilidad que proceda de negligencia es igualmente exigible en el cumplimiento de toda clase de obligaciones; pero podrá moderarse por los Tribunales según los casos".

96 Extrapolando su criterio al ámbito de los contratos de computación en la nube, y en relación a la incidencia de la gratuidad en el ámbito de la relación contractual, nos remitimos a YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet..., op, cit*, pág. 97.

incumpla reiteradamente las políticas de uso adecuado u otras disposiciones contractuales, no abone los pagos devengados, cese su actividad comercial o tras cumplirse un plazo de inactividad en su cuenta[97].

En otras ocasiones, el contrato puede determinar un plazo de duración, a cuyo vencimiento generalmente le sigue una prórroga que se va renovando de manera automática, excepto que se proceda a la voluntad de no renovar por el cliente[98]. Tanto la inclusión en el contrato de unas u otras cláusulas de cancelación del servicio como la suscripción de un eventual pacto de duración determinada dependerán, en gran medida, del objeto del servicio contratado y de la política comercial del proveedor.

En los contratos de computación en la nube pública, objeto de este trabajo, Internet no solo sirve para acceder a la oferta contractual y perfeccionar las cláusulas de adhesión, sino que además permite la ejecución del contrato en el entorno virtual característico del *Cloud Computing*, posibilitando el acceso a los recursos computacionales por el suscriptor de los servicios. Internet permite el acceso inmediato a capacidades informáticas (almacenamiento, procesamiento, funcionalidades de un software...) localizadas en centros de datos remotos, propiedad del proveedor[99]. La banda ancha se convierte así en la vía de transporte de la

97 A modo de ejemplo, podemos observar estas cláusulas en las condiciones generales del servicio *cloud Dropbox para empresas*. <https://www.dropbox.com/es_ES/privacy#business_agreement>. [Fecha de consulta: 25 de febrero de 2016]. Para más detalle, ver Capítulo "Modificación, suspensión y extinción del contrato de computación en la nube".

98 Veamos la cláusula de Google *G-Suite* para empresas respecto al periodo de vigencia del acuerdo suscrito: "10.1. Este Acuerdo tendrá validez durante todo el Periodo de vigencia. 10.2 Periodo de vigencia de los Servicios y adquisiciones durante dicho periodo de vigencia. Google proporcionará los Servicios al Cliente durante el Periodo de vigencia. A menos que las partes acuerden lo contrario por escrito, las Cuentas de usuario final adquiridas durante el Periodo de vigencia de los Servicios tendrán un periodo prorrateado que finalizará el último día de dicho Periodo de vigencia de los Servicios. 10.3 Renovación. a) Plan flexible. Si se adhiere al Plan flexible, el Cliente no se compromete a la adquisición de los Servicios durante un periodo predefinido, sino que abonará los Servicios mensualmente. En consecuencia, no se necesitará ningún evento de renovación para este plan. En su lugar, Google simplemente seguirá facturando los Importes del Cliente en función del uso diario de los Servicios por parte de este último durante el mes anterior. Asimismo, el Cliente podrá cancelar el servicio en cualquier momento. b) Plan anual. Al finalizar cada Periodo de vigencia de los Servicios, los Servicios (y todas las Cuentas de usuario final adquiridas previamente) se renovarán automáticamente por un Periodo de vigencia mensual adicional de los Servicios. Asimismo, después de que el compromiso anual inicial del Cliente haya concluido, el compromiso anual del Cliente cambiará al Plan flexible. Si el Cliente desea renovar el Plan anual, debe cambiar la configuración de renovación en la Consola del administrador para reflejar dicho cambio antes de que termine su compromiso anual". Disponible en: <https://gsuite.google.com/intl/es/terms/2013/1/premier_terms.html>. [Fecha de consulta: 1 de junio de 2017].

99 El proveedor puede ser el propietario de los centros de datos, o subcontratarlos a otro proveedor.

información y los recursos contratados, permitiendo al cliente utilizarlos de igual modo que si efectivamente estuviesen alojados en su propio sistema informático, pudiendo implicar o no la descarga de algún tipo de software en el sistema del cliente como ayuda o soporte para la óptima ejecución del servicio y acceso a la capacidad[100].

4.2.-Naturaleza jurídica del contrato de servicios de computación en la nube pública

De entrada, consideramos adecuado calificar el contrato *cloud* como atípico, aunque lo reconducimos al tipo general de contrato de servicios, puesto que no encaja con otros contratos más específicos que poseen regulación propia y que no recogen satisfactoriamente el conjunto de obligaciones que integra el contrato *cloud*[101]. A continuación, explicamos nuestros criterios sobre la naturaleza del contrato de computación en la nube pública.

4.2.1.- El contrato de computación en la nube como contrato de servicios

Como afirma la doctrina, "desde la perspectiva jurídica, los contratos de servicios pueden y deben identificarse, exclusivamente, a partir de la acepción jurídica del servicio como objeto de la obligación de hacer (arts. 1254, 1271, 1272 y 1274 CC). Consecuentemente, tienen la consideración de contratos de servicios, en sentido jurídico, aquellos en que la prestación o comportamiento que debe realizar uno de los contratantes consiste, fundamentalmente, en el despliegue de cierta actividad intelectual o material"[102].

Por su parte, el Grupo de Trabajo IV sobre contratos electrónicos de la Comisión de Naciones Unidas para el Derecho Mercantil internacional (CNUDMI) ha delimitado la noción los contratos de *Cloud Computing* como contratos de servicios, en los que "una parte (el proveedor de servicios de nube) presta a otra parte (el cliente) servicios de nube que consisten en una o más prestaciones ofrecidas a través de la computación en la nube. Las prestaciones pueden abarcar desde el suministro y el uso de medios de conexión simples y servicios básicos de computación (como almacenamiento de datos, mensajes de correo electrónico o aplicaciones de oficina) hasta el

---

De todos modos, a ojos del cliente, el proveedor será el responsable directo del funcionamiento del total del servicio. Ver apartado "Obligaciones del Proveedor", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

100 Por ejemplo, el software como servicio de almacenamiento *Dropbox* necesita de la descarga de una aplicación en los diferentes dispositivos del cliente para poder proceder a la sincronización automática de los archivos almacenados en la nube.

101 En cuanto a la función modélica del contrato de servicios, nos remitimos a VAQUERO PINTO, Mª José, *Contrato de servicios, op. cit.,* págs. 931 a 965.

102 VAQUERO PINTO, Mª José, *Contrato de servicios, op. cit.*, pág. 934.

suministro y la utilización de toda la gama de recursos físicos y virtuales necesarios para que el cliente elabore sus propias plataformas de tecnología de la información, o para que el cliente despliegue, administre y ejecute aplicaciones o programas informáticos creados o adquiridos por él"[103]. Igualmente, en el mismo texto, la CNUDMI afirma que "Los contratos de servicios de nube son, por lo tanto, una clase especial de contratos de prestación de servicios".

Los contratos de computación en la nube implican para el proveedor *cloud* una serie de actividades que pueden calificarse como servicios, con lo cual las disposiciones sobre compraventa de bienes serían inaplicables, en primer lugar, porque la obligación de computación en la nube se caracteriza por obligaciones de hacer (acceso a la capacidad de manera ininterrumpida, puesta a disposición del cliente de sus contenidos para que pueda recuperarlos, mantener equipos informáticos, actualizar software, implementar medidas de seguridad, etc.) y no en obligaciones consistentes en transmitir el dominio de un objeto (art. 1445 del Código Civil)[104]; y en segundo lugar, porque si bien, y como ya se ha apuntado en anteriores apartados, las capacidades informáticas pueden equipararse a ciertos bienes tangibles y corporales a efectos de aplicar determinadas previsiones normativas, no pueden considerarse equivalentes de tal modo que afecten o determinen la naturaleza jurídica del contrato.

En cuanto a la naturaleza jurídica de los servicios *cloud*, podemos decir que la computación en la nube no se identifica con una única prestación, como bien ha puntualizado, como se ha visto, la CNUDMI, sino que existen diferentes encargos que el proveedor se compromete a ejecutar y que forman el núcleo obligacional de la

103 GRUPO DE TRABAJO IV, CNUDMI, *Aspectos contractuales de la computación en la nube A/CN.9/WG.IV/WP.142* [en línea], pág. 13, disponible en: <http://www.uncitral.org/uncitral/es/commission/working_groups/4Electronic_Commerce.html>. [Fecha de consulta: 1 de junio de 2017]. Recordemos, por otro lado, que este documento forma parte de la preparación de un texto a modo de guía u orientaciones, según lo afirmado en el Acta de la Secretaría, con lo cual la definición del contrato de *Cloud Computing* puede variar una vez finalizados los trámites que den lugar al texto definitivo.

104 Art. 1445 del Código Civil, que recoge en concepto de compraventa: "Por el contrato de compra y venta uno de los contratantes se obliga a entregar una cosa determinada y el otro a pagar por ella un precio cierto, en dinero o signo que lo represente". Como aclaración, también descartamos la compraventa mercantil del artículo 325 del Código de Comercio ("Será mercantil la compraventa de cosas muebles para revenderlas, bien en la misma forma que se compraron, o bien en otra diferente, con ánimo de lucrarse en la reventa") para su aplicación al caso de la computación en la nube, ya que en la inmensa mayoría de casos en los que el contratante es un pequeño empresario, la capacidad contratada no tiene intención de revenderse por el cliente profesional, sino que pretende ser incorporada a su operativa empresarial.

relación contractual, tales como permitir la conectividad externa a la plataforma virtual del proveedor, suministrar la capacidad contratada, custodiar la información que el cliente pueda haber migrado al utilizar el servicio, etc. Por tanto, se tratará, en la inmensa mayoría de casos, de un contrato que, aun coincidente con la esencia del contrato de servicios, superará este concepto y derivará hacia un contrato complejo, al abarcar obligaciones que, si bien en su mayoría son obligaciones de hacer, pueden ser similares o coincidentes con las de otras figuras jurídicas[105].

Por otra parte, y como hemos mencionado, la heterogeneidad de servicios informáticos que pueden ser objeto del contrato únicamente permiten determinar un denominador común que pueda predicarse de este tipo de relaciones jurídicas, quedando un marginal de actividades accesorias que dependerán del concreto diseño de la prestación que realiza el proveedor, de acuerdo con sus propios intereses comerciales. Como veremos en los capítulos pertinentes, muchas de estas obligaciones pueden considerarse obligaciones de medios, en las que el proveedor deberá desplegar su deber de diligencia sin plena garantía de la obtención de un específico resultado, aunque algunas tareas que corresponden al proveedor como ejercicio de su deber de diligencia sean susceptibles de ser calificadas como obligaciones de resultado[106].

105 FERRANTE; Gabriele, "Italian contractual aspects of Cloud Computing", *Comparative Law Yearbook of International Business*, vol. 37, 2015, pág. 127.

106 Las obligaciones de hacer se han venido clasificando por la doctrina como obligaciones de medios y obligaciones de resultado, según la prestación debida (DEMOGUE, R. *Traité des obligations en général*, París, 1925, pàg 538 y ss.). Así, las obligaciones de medios implican un deber de diligencia del deudor, mientras que las obligaciones de resultado añaden a este deber de diligencia la consecución de un resultado determinado como contenido de la prestación. Algunas de las obligaciones del derivadas del contrato *cloud* pueden considerarse obligaciones de medios, mientras que otras se configuran como obligaciones de resultado. El prestador de servicios de *Cloud Computing* pone a disposición del cliente los medios necesarios para que este, a través de su dispositivo con acceso a Internet, pueda acceder a las capacidades y funcionalidades de la infraestructura, plataforma y/o aplicación proporcionadas por el proveedor, convirtiéndose así la prestación del servicio en el núcleo esencial del contrato. El conjunto de obligaciones que lo integran quedarían subsumidas en este, formando parte del servicio. Sin embargo, sobre algunas de las obligaciones esenciales que lo integran, individualmente consideradas, puede sostenerse que se trate de una obligación de resultado, como sucede, concretamente, con la implementación de las concretas medidas de seguridad que den cumplimiento a la normativa de protección de datos de carácter personal. Ver apartado "Obligaciones del proveedor", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

a) La relevancia de la contraprestación del servicio en la determinación de la naturaleza jurídica de los contratos de computación en la nube

En relación a la exigencia de precio cierto, opinamos que no será relevante, para considerar los contratos de computación en la nube como contrato de servicios, el hecho de que, en la mayoría de ocasiones, el precio no esté determinado a tanto alzado en el contrato, sino que dependa de la efectiva utilización de los recursos, a modo de tarifa de consumo.

En aquellos casos en los que el servicio pueda ofertarse a la empresa sin contraprestación dineraria por parte del cliente[107], opinamos que, aun sin existir intercambio pecuniario, raramente se puede considerar el contrato de *Cloud Computing* como contrato gratuito, porque, como hemos observado, el cliente-empresario estará aceptando, a cambio del servicio, contraprestaciones de distinta naturaleza, como soportar publicidad o ceder algún tipo de información[108].

Cuestión diferente es si, tal y como exige la norma legal, el precio integra un elemento esencial del tipo del contrato de servicios o si, por analogía, tales contraprestaciones no económicas u obligaciones de soportar obligan a excluir estos contratos del régimen jurídico que les pueda resultar de aplicación a los contratos *cloud* remunerados dinerariamente. Puede pensarse que la falta de precio determinaría que el contrato de computación en la nube no pudiera calificarse como contrato de servicios, desviando su regulación hacia otras figuras de carácter gratuito que pudieran ser similares, como el comodato o el simple préstamo del art. 1740 del Código Civil. En nuestra opinión, carece de sentido hablar de comodato respecto de una capacidad informática, ya que debe tener por objeto un bien no consumible, para que pueda ser restituido. Del mismo modo, el simple préstamo tampoco encaja con el diseño del contrato de computación en la nube, puesto que el cliente *cloud* no adquiere la titularidad de las capacidades suministradas, ni está obligado a devolver lo consumido en igual cantidad o calidad (arts. 1753 y siguientes del Código Civil)[109].

---

107 Queremos dejar constancia de que, en la práctica, si bien son frecuentes los servicios proporcionados gratuitamente a particulares, a cambio de soportar anuncios publicitarios o de ceder sus datos personales a terceros, son más bien escasas las ocasiones en las que se ofrece esta opción a empresarios y profesionales que se identifiquen ante el proveedor como tales.

108 Ver apartado "Contrato oneroso", en este mismo capítulo.

109 En el informe final para la Comisión Europea *Comparative Study on Cloud Computing Contracts,* los expertos de diferentes países en general clasifican el contrato de computación en la

En nuestra opinión, y como reiteraremos más adelante, el contrato de computación en la nube para pequeños y medianos empresarios generalmente está sujeto a precio, o, en ciertos casos, sujeto a contraprestaciones de naturaleza no dineraria, con lo cual raramente será gratuito. Aun así, coincidimos con otros autores al determinar que la falta de contraprestación dineraria, como elemento integrante del tipo, no es razón suficiente para afirmar la falta de fuerza obligatoria entre las partes[110].

Si, como vemos, ya presenta dificultades la determinación de la naturaleza jurídica en cuanto a los servicios de computación en la nube generalmente considerados, la tarea no se simplifica al adentrarnos en los pormenores resultantes de sus categorizaciones. A continuación, presentamos nuestras propuestas de acuerdo con la opción de contratación en el modelo de implementación de la nube pública y sus principales tipos de servicio (infraestructura, plataforma y software como servicio).

b) La relevancia de las diferentes modalidades de implementación en la determinación de la naturaleza jurídica de los contratos de computación en la nube

Hemos expuesto en el capítulo anterior que existen diferentes modelos de implementación de la nube: privada, híbrida, comunitaria y pública. La nube pública

---

nube como un contrato de servicios. Por otra parte, los letrados alemanes consideran equiparable al comodato o al simple préstamo (en concreto, a las figuras equivalentes en su ordenamiento jurídico) aquellos servicios de computación en la nube que se prestan de manera gratuita. Como hemos manifestado en diferentes apartados de este capítulo, no compartimos esta opinión, en primer lugar, porque consideramos que no pueden considerarse contratos de computación en la nube gratuitos, puesto que siempre suelen existir contraprestaciones no dinerarias que debe realizar el cliente para acceder al servicio, y por tanto, al ser el comodato un contrato en esencia gratuito, no cabría compararlo con el contrato de computación en la nube (art. 1740 del Código Civil:"Por el contrato de préstamo, una de las partes entrega a la otra, o alguna cosa no fungible para que use de ella por cierto tiempo y se la devuelva, en cuyo caso se llama comodato, o dinero u otra cosa fungible, con condición de devolver otro tanto de la misma especie y calidad, en cuyo caso conserva simplemente el nombre de préstamo. El comodato es esencialmente gratuito. El simple préstamo puede ser gratuito o con pacto de pagar interés"; 1753 del Código Civil: "El que recibe en préstamo dinero u otra cosa fungible, adquiere su propiedad, y está obligado a devolver al acreedor otro tanto de la misma especie y calidad"). En segundo lugar, porque creemos que la falta de precio no es motivo suficiente como para determinar una diferente concepción de la naturaleza jurídica entre dos contratos cuyas prestaciones principales sean equivalentes. COMISIÓN EUROPEA. *Final Report for Comparative Study on Cloud Computing Contracts* [en línea], 2015. Disponible en: <http://bookshop.europa.eu/en/comparative-study-on-cloud-computing-contracts-pbDS0115164/>. [Fecha de consulta: 11 de abril de 2017].

110 YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet, op. cit., pág*. 91.

se caracteriza por su posibilidad de contratación por el público en general (independientemente del concreto mercado al cual se dirija el producto), y se contrata mediante condiciones generales y en línea, de manera no negociada y masificada. Por contra, el modelo de nube híbrida, si bien igualmente puede contratarse del mismo modo, permite un mayor margen de personalización del diseño del servicio por parte del proveedor, y puede posibilitar negociaciones bilaterales y el establecimiento de pactos consensuados entre ambas partes.

Por tanto, los contratos de nube privada, comunitaria y (en ciertos casos) híbrida, integran contenidos más flexibles y posiblemente negociados, con lo cual pueden implicar una diferente configuración de obligaciones entre ambas partes (y una distinta distribución de riesgos y responsabilidades)[111]. Sin embargo, estos aspectos no afectarán a su común naturaleza jurídica: el contrato de servicios, ya que coinciden en la prestación en torno a la cual giran estos contratos: la puesta a disposición en línea de capacidades informáticas[112].

A partir de lo anterior, consideramos que, aun correspondiéndose con la misma naturaleza jurídica (contrato de servicios), pueden existir diferentes contenidos obligacionales de acuerdo con la modalidad de implementación escogida, variándose el contenido de las obligaciones que consideramos principales en el contrato de nube pública[113].

Por ello, debido a las diferencias existentes entre los diferentes modelos de implementación, consideramos difícil establecer un concepto de contrato de computación en la nube unívoco capaz de englobar de manera válida todos los contenidos que puedan alcanzar los diferentes modelos de implementación, especialmente aquellos que las partes negociarán libremente, aunque coincidan en el acceso ininterrumpido en línea a capacidades informáticas como una de sus prestaciones primordiales.

---

111 Por ejemplo, hemos comentado como la nube privada es muy similar al *Outsourcing* informático.

112 Ello tampoco obsta para que muchas de las cuestiones analizadas en este trabajo sean igualmente extensibles a condiciones de contratos negociados.

113 Recordemos que, por ejemplo, la nube privada puede incluso utilizar el hardware de la propia empresa cliente, hecho que afectará de manera singular a las obligaciones de seguridad, las cuales no podrán equipararse a las que debe asumir un proveedor de nube pública, sino que serán más similares a las de un contrato de *Outsourcing* informático. Ver capítulo "Concepto y características técnicas de la computación en la nube".

A pesar de lo anterior, consideramos factible determinar una definición de contrato de servicios de computación en la nube pública, así como un abanico general de obligaciones que comparten los servicios *cloud* de implementación pública a través de condiciones generales de la contratación, que realizaremos al final de este capítulo. Además de estas obligaciones principales, cabrán otras obligaciones accesorias que vendrán determinadas por el propio objeto del contrato y dependerán de la estrategia comercial de cada proveedor *cloud*. Para un análisis pormenorizado, nos remitimos al capítulo de este trabajo dedicado a tal efecto[114].

c) La relevancia de la personalización del servicio y de los diferentes tipos de servicio en la determinación de la naturaleza jurídica de los contratos de computación en la nube

El aprovisionamiento de estas capacidades de infraestructura, plataforma o aplicaciones, como se ha dicho, no implica la transmisión de la titularidad de activos del proveedor, (es decir, el proveedor no transfiere la titularidad de equipos hardware o los derechos sobre programas informáticos), sino la puesta a disposición del cliente de estas capacidades por medios electrónicos. El cliente, a través del pago (o de otras contraprestaciones no dinerarias) quedará habilitado para su uso.

En entornos de nube pública, este uso del recurso o capacidad no es exclusivo, sino que se comparte con otros clientes del proveedor que usan el servicio y comparten infraestructuras. Por ello, la personalización de la capacidad informática y su adaptación a las necesidades del cliente se lleva a cabo a través del propio diseño del producto informático y de su interfaz, que permite la configuración de determinados aspectos por parte del cliente, a modo de autoservicio. Por tanto, al no llevarse a cabo por el proveedor como una tarea o encargo esta personalización, excluye que el contrato de computación en la nube pública sea asimilable a un contrato de ejecución de obra (art. 1544 del Código Civil)[115], ya que tanto servicio como capacidad se ofertan con unas características o funcionalidades determinadas, a modo de *"Utility Computing*", es decir, susceptible de comercializarse como un bien de consumo estándar[116].

---

114 Ver capítulo "Obligaciones y Responsabilidades de las partes del contrato de computación en la nube".

115 Art. 1544 Código Civil: "En el arrendamiento de obras o servicios, una de las partes se obliga a ejecutar una obra o a prestar a la otra un servicio por precio cierto".

116 En aquellos casos en los que el contrato implicase la obligación del proveedor de realizar

Algunos contratos de computación en la nube, especialmente aquellos que tienen por objeto capacidades de infraestructura o plataforma, en los que el proveedor pone a disposición del cliente espacio de almacenamiento digital en sus equipos y servidores o el uso de máquinas virtuales, pueden plantear la cuestión de su calificación como contratos de arrendamiento de cosas (art. 1543 del Código Civil[117]), aunque para ello deberá contemplarse el conjunto de obligaciones que integran la prestación del proveedor. A nuestro parecer, aunque esta apreciación sería jurídicamente defendible (ya que el arrendamiento tampoco supone la transmisión del dominio de aquello arrendado), cabe realizar algunos matices. En primer lugar, debe estarse a la cuestión de si el espacio virtual ubicado en servidores remotos puede calificarse jurídicamente como "cosa", ya que el hecho de facilitar al cliente capacidades informáticas no implica el arrendamiento del hardware involucrado (cableado, servidores donde se almacenan los datos, plataforma o aplicación, etc.).

En segundo lugar, esta figura jurídica no alcanzará, en muchos casos, todas las obligaciones que integran el contrato de computación en la nube, ni tampoco podría predicarse de todos los servicios de infraestructura o plataforma, sino únicamente de aquellos que consisten en la cesión de un espacio digital cuyo "arrendatario" posea gran parte del control y administración, y que restrinja el papel del propietario de la nube al mantenimiento del equipo en funcionamiento. Así, deberán distribuirse entre ambos las obligaciones de custodia de contenidos, dependiendo del nivel de control y configuración de los sistemas de seguridad de cada una de las partes, obligaciones no predicables de los contratos de arrendamiento tradicionales. Igualmente, el propietario no solo estaría "alquilando" el espacio del servidor remoto, sino que también estaría realizando otras cesiones, como los derechos de uso del sistema operativo que permite controlarlo.

Por otra parte, la similitud del contrato de computación en la nube al

---

ciertos ajustes de personalización del servicio para un determinado cliente, como sucede en los modelos de implementación de nube privada o comunitaria de nube, podrían aplicarse las disposiciones relativas al contrato de obra, aunque para determinar su naturaleza como contrato de obra deberá atenderse al contenido global del contrato y al peso de esta obligación de personalización dentro del conjunto de obligaciones contractuales. En cuanto al concepto de "*Utility Computing*", nos remitimos al capítulo "Concepto y características técnicas de la computación en la nube".

117 Art. 1543 del Código Civil: "En el arrendamiento de cosas, una de las partes se obliga a dar a la otra el goce o uso de una cosa por tiempo determinado y precio cierto".

contrato de arrendamiento únicamente puede predicarse de ciertos contratos de computación en la nube. Por ejemplo, muchos de los contratos del tipo software como servicio, como se ha mencionado, son más cercanos a las licencias de uso y al contrato de prestación de servicios que al arrendamiento de cosas, como las redes sociales o el correo electrónico.

Por nuestra parte, nos decantamos por una perspectiva más integradora, y creemos oportuno considerar los servicios de infraestructura y plataforma de una manera que permita incorporarlos, junto con el software como servicio, dentro del concepto global de contratos de servicios de computación en la nube. Todo ello con la finalidad de que todos estos contratos reciban un tratamiento jurídico unitario, puesto que tanto unos como otros, además de compartir los fundamentos informáticos y técnicos de la arquitectura en capas, coinciden en su prestación esencial: la puesta a disposición en línea de capacidades informáticas. Todo ello independientemente de cuál sea la concreta capacidad informática facilitada (almacenamiento remoto, procesamiento, funcionalidades de software u otras), del mayor o menor grado de control y gestión por parte del cliente (el cual dependerá del diseño del servicio por el proveedor), y de la distribución de obligaciones y responsabilidades entre las partes (las cuales dependerán de la configuración de las condiciones generales predispuestas), puesto que las obligaciones propias del contrato serán, en esencia, coincidentes.

Todos estos aspectos pueden suponer *a posteriori* diferencias entre unos y otros contratos, como contratos complejos que son (como veremos en posteriores apartados), aunque, en nuestra opinión, tales diferencias no son suficientes como para motivar la realización de distinciones en cuanto a su naturaleza jurídica, que es única. Son todos ellos, a nuestro parecer, contratos de prestación de servicios.

4.2.2.-El contrato de computación en la nube como contrato atípico

El principio general de la libre contratación permite a las partes negociar y establecer acuerdos sin necesidad de ajustarse a las figuras jurídicas legalmente previstas, y adecuar a sus intereses los pactos que suscriban[118] Por nuestra parte, no hemos encontrado en la normativa española regulación del contrato de servicios de

118 DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. I. Introducción. Teoría del contrato*, 6ª Edición, Navarra, 2007, pág. 487.

computación en la nube, con lo cual podemos afirmar que se trata de un contrato atípico[119], carente de regulación específica, que puede reconducirse al genérico contrato de servicios[120]. Así, coincidimos plenamente con lo afirmado por APARICIO VAQUERO respecto del contrato de *Outsourcing* como arrendamiento de servicios, y haciéndolo extensible también a los contratos de computación en la nube: "Lo curioso es que, aun concediendo al *Outsourcing*, [y añadimos, en nuestro caso, a los contratos de computación en la nube pública] en abstracto, el carácter de arrendamiento de servicios, dada la escasa regulación que nuestro Código Civil hace de él, es posible considerarlo «atípico» en cierta medida, con lo que habría que estar en todo caso a lo acordado por las partes y, en lo no acordado por ellas, a las reglas generales sobre obligaciones y contratos, contempladas bajo el interés de las partes"[121].

En cuanto a su regulación, consideramos que, si bien las prestaciones propias de los contratos *cloud* pueden corresponderse, individualmente consideradas, con las de otras figuras jurídicas tipificadas, lo cierto es que el conjunto del servicio *cloud* excede de las limitaciones particulares que presentan tales figuras, siendo necesario acudir, en caso de conflicto, en primer lugar, a lo establecido contractualmente[122], en virtud de la autonomía de la voluntad y del principio *pacta sunt servanda* (arts. 1091 y 1255 del Código Civil, respectivamente) y, a falta de pacto, a la tipología genérica, esto es, el contrato de servicios, por ser la obligación principal el acceso ininterrumpido a los recursos de forma elástica desde dispositivos con conexión a Internet(arts. 1544 y 1583 a 1587 del Código Civil).

Estas disposiciones legales deben combinarse con las disposiciones de otras figuras jurídicas, que pueden aplicarse de forma analógica a concretas obligaciones contractuales con las cuales comparten rasgos esenciales (por ejemplo, el depósito en relación a la obligación del proveedor *cloud* de custodiar los datos migrados, el suministro en cuanto a la disponibilidad de acceso, etc.), puesto que el contrato de

119 Tomamos como referencia la definición que realiza DIEZ-PICAZO del contrato atípico como "*aquel que carece de reconocimiento legal y de disciplina normativa*". DIEZ-PICAZO, Luís, *Fundamentos..., op. cit,* pág. 447.

120 Ver apartado "El contrato de computación en la nube como contrato complejo", en este mismo capítulo.

121 APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática..., op. cit.*, pág. 71.

122 El principio *pacta sunt servanda* aparece recogido en el artículo 1091 del Código Civil ("Las obligaciones que nacen de los contratos tienen fuerza de ley entre las partes contratantes, y deben cumplirse a tenor de los mismos"), y la libertad de pacto, en el artículo 1255 del Código Civil ("Los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público").

computación en la nube es, como se verá, un contrato complejo o mixto[123]. De forma subsidiaria, serán de aplicación los principios generales de las normas sobre obligaciones y contratos, informados por la buena fe contractual (arts. 1258 del Código Civil y 58 del Código de Comercio[124]) y los usos comerciales del sector (art. 2 del Código de Comercio[125]).

4.2.3.- El contrato de computación en la nube como contrato complejo

Finalmente, podríamos hablar del contrato *cloud* como contrato mixto o complejo[126] puesto que entendemos que combina obligaciones correspondientes a contratos típicos ya existentes (como el contrato de servicios o el depósito) y a otras figuras habituales en el tráfico mercantil (suministro mercantil, *Hosting*, etc.), como ya se ha observado en este mismo capítulo[127].

4.3.- Definición jurídica del contrato de computación en la nube de implementación pública

De lo expuesto hasta el momento se desprende la dificultad de establecer una definición que pueda abarcar los distintos servicios de nube pública: infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS). Aunque todos estos contratos se sustentan en entornos informáticos similares, (o incluso coincidentes), la falta de homogeneidad en su objeto complica decantarse

123 El contrato mixto combina diferentes tipos contractuales o varias prestaciones singulares reguladas en diferentes tipos regulados en el ordenamiento, y deben juzgarse, en todo aquello no determinado por la voluntad contractual, por analogía de los tipos contractuales más afines, por los principios generales de las obligaciones y por los principios generales del Derecho. CASTÁN TOBEÑAS, José; *Derecho Civil Español, común y foral,* 15ª edición, Madrid, 1993, pág. 19.

124 Art. 1258 del Código Civil: "Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan, no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley". Artículo 58 del Código de Comercio: "Los contratos de comercio se ejecutarán y cumplirán de buena fe, según los términos en que fueren hechos y redactados, sin tergiversar con interpretaciones arbitrarias el sentido recto, propio y usual de las palabras dichas o escritas, ni restringir los efectos que naturalmente se deriven del modo con que los contratantes hubieren explicado su voluntad y contraído sus obligaciones. ".

125 Artículo 2 del Código de Comercio: "Los actos de comercio, sean o no comerciantes los que los ejecuten, y estén o no especificados en este Código, se regirán por las disposiciones contenidas en él; en su defecto, por los usos del comercio observados generalmente en cada plaza, y, a falta de ambas reglas, por las del Derecho común. (...)":

126 DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. I. Introducción. Teoría del contrato*, 6ª Edición, Navarra, 2007, pág. 490. CASTÁN TOBEÑAS, José*; op. cit.*, pág. 19. FERRANTE; Gabriele, *op. cit.,* págs. 127 a 147.

127 Ver apartado "Figuras afines al contrato de computación en la nube", en este mismo capítulo.

por una definición que refleje los matices de cada uno[128].

Igualmente, además del objeto contractual, existen otras variables que pueden provocar diferencias en contratos de servicios *cloud* con prestaciones similares, como son la orientación del servicio para su suscripción por empresarios o por consumidores, la existencia o no de contraprestación dineraria o los propios intereses comerciales del proveedor, etc. Así, estos factores pueden afectar, entre otros aspectos, a la distribución de responsabilidades entre las partes, a la mayor o menor intensidad del deber de colaboración mutua y a la existencia de obligaciones accesorias.

Siendo conscientes de estas dificultades, consideramos conveniente, e incluso necesario, finalizar este capítulo con una definición que permita delimitar el contenido general de estos contratos, atendiendo a las obligaciones preponderantes asumidas generalmente por las partes y que consideramos inherentes del contrato de computación en la nube pública.

Por ello, efectuadas las consideraciones anteriores, definimos el contrato de computación en la nube pública como aquel contrato de servicios en el cual el proveedor se compromete a proporcionar acceso continuado, ininterrumpido y a través de medios o canales electrónicos a recursos computacionales consistentes en capacidades de infraestructura, plataformas para el desarrollo de programas y/o aplicaciones software, ajustándose a la demanda puntual del cliente y permitiéndole la autogestión del uso de esos recursos, así como a implementar las medidas de seguridad que le permitan custodiar y devolver en formato útil los datos digitales que el cliente, en el uso de esos servicios, le pueda confiar; y el cliente, por su parte, se compromete a retribuir el consumo que realiza de estos servicios de acuerdo con lo suscrito y a hacer un uso adecuado de los recursos que el proveedor pone a su disposición.

128 Un mismo entorno *cloud* puede soportar servicios de las tres categorías. Ver capitulo "Concepto y características técnicas de la computación en la nube".

Capítulo Tercero

ELEMENTOS SUBJETIVOS DEL CONTRATO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE PÚBLICA

1.- INTRODUCCIÓN

En los contratos de servicios de *Cloud Computing* participan múltiples actores, aunque no todos ellos pueden considerarse partes del contrato entre proveedor (empresario que presta el servicio) y cliente (quien lo demanda), como veremos a continuación.

Es frecuente que, ante el cliente, el servicio que se ofrece tenga la apariencia de ser unitario, y que, sin embargo, subyazcan diferentes subcontrataciones. Ello sucede especialmente en prestaciones de software como servicio (SaaS), ofertadas por empresas de pequeño o mediano tamaño y que se sustentan en servicios de *Hosting* o de plataforma o infraestructura *cloud* subcontratados a terceros proveedores[1]. De la correcta prestación de estos servicios subcontratados puede depender el cumplimiento de lo acordado contractualmente con el cliente final.

Por otra parte, la dimensión económica de los contratantes incide

1 MARCHINI, Renzo; *Cloud Computing: a practical introduction to the legal issues,* 1ª edición, Londres, 2010, pág. 104.

considerablemente en la negociación contractual. En general, los proveedores únicamente consienten entablar una negociación presencial ante grandes empresas o clientes estratégicos[2], negociación en la cual procuran adaptarse a las exigencias específicas necesarias para captar al cliente. Cabe decir que los resultados de estas negociaciones se hacen públicos en muy pocas ocasiones[3]. En cambio, la contratación de servicios *cloud* por parte de particulares y pequeños empresarios tiene lugar mayoritariamente con la suscripción de condiciones generales, a menudo a través de formularios en línea[4]. Este sistema facilita al proveedor la oferta en masa de paquetes de servicios computacionales idénticos para todos sus clientes, quienes, a su vez, pueden contratar estos servicios de forma individual o combinados, según sean las necesidades informáticas a cubrir[5].

Teniendo en cuenta que son pocos los pequeños empresarios que pueden permitirse un servicio *cloud* personalizado con su presupuesto, la mayoría deberá acudir a servicios comercializados en línea y elegir entre las distintas ofertas cuál es la que mejor se adapta a sus necesidades. La toma de contacto entre las partes suele tener lugar con la introducción de los datos del demandante del servicio en el sitio web del proveedor, donde normalmente se identificará como particular o empresa.

---

2 Por ejemplo, ciertas Administraciones Públicas o entidades bancarias. BRADSHAW, Simon; MILLARD, Christopher; WALDEN, IAN; "Standard contracts for Cloud Computing Services", *Cloud Computing Law,* 1ª edición, Oxford, 2013, págs. 37 a 39.

3 Así lo afirman, en su estudio comparativo de contratos de computación en la nube, BRADSHAW, Simon; MILLARD, Christopher; WALDEN, IAN*, op. cit.*, pág. 39.

4 Atendiendo a la Exposición de Motivos de la Ley 17/1998 sobre Condiciones Generales, es condición general: "una cláusula es condición general cuando está predispuesta e incorporada a una pluralidad de contratos exclusivamente por una de las partes (…) Las condiciones generales de la contratación se pueden dar tanto en las relaciones de profesionales entre sí como de éstos con los consumidores. En uno y otro caso, se exige que las condiciones generales formen parte del contrato, sean conocidas o -en ciertos casos de contratación no escrita- exista posibilidad real de ser conocidas, y que se redacten de forma transparente, con claridad, concreción y sencillez. Pero, además, se exige, cuando se contrata con un consumidor, que no sean abusivas". Así, se diferencia de una cláusula abusiva en que esta es, como dice la misma Exposición, "la que en contra de las exigencias de la buena fe causa en detrimento del consumidor un desequilibrio importante e injustificado de las obligaciones contractuales y puede tener o no el carácter de condición general, ya que también puede darse en contratos particulares cuando no existe negociación individual de sus cláusulas, esto es, en contratos de adhesión particulares".

5 Estos "paquetes" o "lotes" están conformados por un servicio principal y varios servicios accesorios, o por varios servicios complementarios entre sí. A modo de ejemplo, la web de *Google* permite al cliente combinar servicios propios de la nube (de computación como *App Engine* o *Compute Engine*; y almacenamiento como *Cloud Storage* o *Cloud SQL*) y servicios accesorios (como el análisis de *Big Data* con la herramienta *BigQuery;* o la traducción de las aplicaciones a múltiples idiomas con el traductor *Translate API*). Disponible en: <https://cloud.google.com/products/>. [Fecha de consulta: 19 de abril de 2017].

En ocasiones, el diseño de la página web proporciona otras formas más interactivas de presentación entre las partes a iniciativa del proveedor, como los "videochats" con personal comercial o la publicación en la web de un teléfono gratuito para solicitar información sobre los servicios[6]. Los blogs y foros en línea especializados con opiniones de otros usuarios[7] pueden completar la información al interesado en contratar servicios *cloud*[8].

En este capítulo, estudiaremos el papel que desempeña cada una de las partes del contrato y la interacción entre ellas, las principales normas españolas que resultan de aplicación como consecuencia de esa contratación (Ley de Servicios de la Sociedad de la Información, Ley de Ordenación del Comercio Minorista, normativa de protección al consumidor, etc.) así como la concurrencia de terceros que pueda afectar, de uno u otro modo, a la distribución de responsabilidades ante terceros. Prestaremos especial atención al pequeño empresario suscriptor de servicios de computación en la nube, por ser el objeto principal de este trabajo, sin perjuicio de eventuales referencias a la contratación por consumidores o entidades públicas.

---

6 La web del software como servicio de almacenamiento *Dropbox para empresas* ofrece al cliente entablar una conversación mediante mensajes electrónicos en línea. En cambio, la web de *Microsoft Azure* nos facilita un teléfono para contactar con el departamento de ventas y un formulario para efectuar consultas. Disponibles respectivamente en: <https://www.dropbox.com/business/why-dropbox-for-business> y <http://azure.microsoft.com/es-es/>. [Fecha de consulta:19 de abril de 2017].

7 En este trabajo, nos referiremos al "usuario" de servicios atendiendo a la acepción segunda del Diccionario de la Lengua Española en su 22ª edición: "dicho de una persona: que tiene derecho de usar de una cosa ajena con cierta limitación", y entendiendo que puede ser una persona física o jurídica que utilice el servicio, independientemente de que ese uso tenga lugar en el marco de una actividad empresarial o profesional. Así, emplearemos esta acepción del término usuario, y no el término "usuario" como equivalente a "consumidor", recogido en el artículo 3 de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias ("A efectos de esta norma y sin perjuicio de lo dispuesto expresamente en sus libros tercero y cuarto, son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión. 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"). Por otra parte, como veremos más adelante, el término "usuario" no siempre coincide con el de "contratante de servicios *cloud*", como sucede cuando un empleado hace uso de los servicios *cloud* que ha suscrito la empresa en la que trabaja. Igualmente, consideramos la distinción entre cliente y usuario de los servicios importante en cuanto a la determinación de responsabilidades por uso, como se estudiará en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

8 Será información complementaria a la que pueda proporcionar el propio proveedor. Ver apartado "La responsabilidad del proveedor por la adaptabilidad del servicio a las necesidades del cliente y su relación con el deber de información precontractual", en el capítulo Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

2.- EL PROVEEDOR DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

Consideramos proveedor de servicios de computación en la nube al empresario que presta estos servicios de manera profesional, a cambio de un precio u otra contraprestación no monetaria que igualmente le suponga interés comercial[9].

Si nos detenemos a examinar la situación del mercado empresarial de los proveedores de servicios tecnológico-informáticos, cabe decir que el aprovisionamiento en línea de capacidades informáticas ha favorecido la aparición de una nueva diversidad de empresas en el sector. Los proveedores líderes son propietarios de grandes centros de procesamiento de datos, esto es, conjuntos de sistemas hardware y software que contienen los recursos informáticos para procesar la información de una organización[10]. De esta manera, se aprovechan los excedentes de capacidad informática de sus propios centros de datos y los suministran a clientes cuyas necesidades computacionales son menos complejas y deben cubrirse a corto plazo[11]. El abanico de proveedores abarca desde multinacionales que comercializan servicios *cloud* en general a pequeños proveedores de software como servicio. Los grandes proveedores suministran servicios de computación no personalizados y totalmente automatizados, promoviendo su consumo en masa, con un bajo coste de administración y mantenimiento de la infraestructura[12], a precios muy competitivos,

9 Para más detalle, ver ROSSELLÓ RUBERT, Fca. M, "Las contraprestaciones no dinerarias en la Propuesta de Directiva sobre suministro de contenidos digitales", *Revista de Derecho Mercantil,* núm. 303, 2017, págs. 163 a 190. Asimismo, ver apartado "Características de los contratos de servicios de computación en la nube: Contrato oneroso" en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

10 Como ejemplos de grandes proveedores de servicios de computación en la nube, podemos mencionar Google, Amazon o Microsoft, que ofrecen servicios de infraestructura, plataforma y software. Además, son muchas las empresas europeas que operan en el mercado, como T-Systems (filial de Dutsche Telekom) o Telefónica como prestadores de infraestructura. Cuando nos adentramos en la prestación de servicios software, el número de proveedores que opera en el mercado se dispara, al ser servicios muy diversos y de creación y salida al mercado más sencillas, puesto que requieren una menor inversión por parte del proveedor.

11 Amazon es una compañía americana dedicada al comercio electrónico que decidió en 2002 "alquilar" los excedentes de capacidad de sus centros de datos. En 2006 nace oficialmente Amazon Web Services, y actualmente es uno de los proveedores internacionales de servicios de computación en la nube más importantes, junto con Microsoft y Google. Fuente: *Gartner's Magic Quadrant for Cloud Infrastructure as a Service, Worldwide*, 2016 [en línea]. Disponible en <https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519>. [Fecha de consulta: 19 de abril de 2017]

12 BBVA OBSERVATORIO DE ECONOMÍA DIGITAL, *El desarrollo de la industria del Cloud*

y obteniendo grandes beneficios debido a las economías de escala, pudiendo combinar los servicios *cloud* con otros productos y servicios tecnológicos dentro de extensos catálogos[13].

Muchos de los suscriptores de servicios de estos grandes proveedores son, a su vez, empresas de menores dimensiones que proporcionan software como servicio a sus propios clientes y a consumidores. De esta manera se sirven de la infraestructura, plataforma u otro software proporcionado por terceros proveedores, ahorrándose la inversión y el mantenimiento de centros de datos propios para desarrollar o soportar el software que ellas mismas proveen. Nos encontramos, pues, ante diferentes tipos de proveedores de servicios *cloud*, y como hemos visto, algunos de ellos pueden depender de los recursos computacionales suministrados por otros, o pueden ser titulares de sus propios centros de datos[14].

Sea propietario o no de su propia infraestructura, la función principal del proveedor de servicios de computación en la nube es permitir el acceso a sus clientes a los recursos informáticos contratados, disponibles a través de Internet[15]. La relación entre proveedor y cliente se materializará a través del contrato de servicios *cloud,* que tendrá lugar mediante contratación electrónica[16].

De este modo, el proveedor ofrecerá uno u otro prototipo de contrato dependiendo de la categoría del cliente, siendo habitual que solo se permita

---

Computing: impactos y transformaciones en marcha [en línea], 2014, pág. 2. Disponible en: <https://www.bbvaresearch.com/publicaciones/el-desarrollo-de-la-industria-del-cloud-computing-impactos-y-transformaciones-en-marcha/>. [Fecha de consulta: 2 de agosto de 2016].

13 Google, proveedor de servicios tecnológicos, no solo ofrece soluciones *cloud* como la infraestructura como servicio (IaaS) *Google Compute Engine*, la plataforma como servicio *Google App Engine* o los softwares como servicio (SaaS) de *Google G-Suite.* En su amplia oferta de servicios y productos, también podemos encontrar otras soluciones para empresas, como su servicio de publicidad (*Google AdWords*), herramientas de análisis de tráfico de sitios web (*Google Analytics*) o el buscador para empresas *Google Search Appliance*. Disponible en: <http://www.google.es/intl/es/services/sitemap.html>. [Fecha de consulta: 19 de abril de 2017].

14 Los aspectos contractuales relacionados con la subcontratación son relevantes en relación a las responsabilidades derivadas de la prestación del servicio y en cuanto al cumplimiento de la normativa en materia de protección de datos, como podrá observarse de manera más detallada en el apartado "La responsabilidad del proveedor por actuaciones de los subproveedores", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

15 Para más detalle sobre las obligaciones del proveedor *cloud*, ver capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

16 Ver apartado "Características de los contratos de servicios de computación en la nube: Contrato consensual", en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

negociación de las cláusulas a empresas de grandes dimensiones o Administraciones Públicas. Independientemente de que se someta o no a negociación posterior, este documento suele contener por defecto un clausulado más protector de los intereses del propio proveedor, ya que disfruta de una posición dominante en la relación contractual al ser quien redacta, al menos inicialmente, los contenidos de la relación obligacional.

La contratación de servicios *cloud* por pequeños empresarios, en los cuales se centra este trabajo, mayoritariamente tendrá lugar a través de la suscripción de condiciones generales, las cuales, además de ser redactadas íntegramente por el proveedor, serán innegociables, quedándole como única alternativa al cliente disconforme la no suscripción del contrato y la búsqueda de un proveedor alternativo. En apartados posteriores de este mismo capítulo analizaremos las cuestiones jurídicas relacionadas con el cliente pequeño empresario suscriptor de servicios de computación en la nube pública, objeto de este trabajo, sin perjuicio de que algunas de las afirmaciones puedan hacerse extensibles a contratos suscritos por consumidores u organismos públicos.

2.1.- El proveedor de servicios en la nube como prestador de servicios de la sociedad de la información

El hecho de considerar al proveedor de servicios *cloud* como prestador de servicios de la sociedad de la información a efectos de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (en adelante, LSSI) tendrá consecuencias jurídicas importantes. En concreto, estará sometido a las obligaciones que la propia Ley establece: entre otras, las relativas a información general (art. 10), comunicaciones comerciales (arts.19 a 22) y contratación electrónica (arts. 23 a 29).

Para determinar si el proveedor de servicios de computación remota puede considerarse prestador de servicios de la sociedad de la información, en primer lugar analizaremos si los servicios *cloud* pueden considerarse "servicios de la sociedad de la información" según el ámbito objetivo de aplicación de la LSSI[17].

En su Exposición de Motivos, la LSSI afirma que el concepto de servicio de

17 En relación a por qué se considera un servicio y no una obra o producto, ver capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

sociedad de la información tiene un sentido amplio, que engloba: a) la contratación electrónica de bienes y servicios, b) el suministro de información en línea, y c) las actividades de intermediación.

En primer lugar, en la medida en que los servicios de computación en la nube se contraten electrónicamente, podemos afirmar, conforme a lo mencionado por la Ley, que son un servicio de la sociedad de la información[18].

En segundo lugar, atendiendo al sentido amplio del concepto "servicio de la sociedad de la información" que recoge la propia Exposición de Motivos de la LSSI, en aquellos casos en los cuales la contratación tuviera lugar *offline*, opinamos igualmente que el suministro de herramientas computacionales a través de la red posibilita una interpretación extensiva de la expresión "suministro de información en línea", y que el suministro de contenidos en línea forma parte del abanico de servicios ofrecidos por los proveedores *cloud*.

En tercer lugar, debemos añadir que, independientemente de que la contratación se realice o no electrónicamente, en las definiciones recogidas en el Anexo de la LSSI, se considera servicio de la sociedad de la información "todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario". Aunque hemos comentado que los servicios de computación en la nube son gestionados por el usuario a modo de autoservicio[19], no cabe duda de que su prestación se realiza a través de la red y a distancia: los centros de datos dispersos geográficamente generan los recursos de infraestructura, plataforma y software (esto es, IaaS, PaaS o SaaS) contratados; y el usuario accede a tales contenidos, por ejemplo, mediante el acceso autenticado a una interfaz del sitio web del proveedor[20].

Por último, cabe destacar que no es necesario que el servicio deba ser retribuido para ser considerado servicio de la sociedad de la información. La LSSI especifica que también son servicios de la sociedad de la información aquellos "no remunerados por sus destinatarios, en la medida que constituyan una actividad económica para el prestador de servicios". De este modo, son servicios de la sociedad de la información aquellos servicios sin contraprestación dineraria por parte del cliente, como las redes sociales,

18 Ello sucede en la inmensa mayoría de contrataciones, especialmente cuando quien suscribe el contrato como cliente es una pequeña empresa.

19 Ver capítulo "Concepto y características técnicas de la computación en la nube".

20 Ver apartado "Características de los contratos de servicios de computación en la nube", en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

o servicios de correo electrónico o de software de almacenamiento limitado[21]. Ello no implica, como se ha visto, que estos servicios puedan considerarse carentes de onerosidad[22].

Una vez clasificado el servicio *cloud* como servicio de la sociedad de la información, debemos plantearnos si es, además, categorizable como servicio de intermediación. De ser así, deberá cumplir con las obligaciones añadidas que la Ley impone a estos prestadores, en especial, el deber de colaboración del art.11[23], las obligaciones sobre información de seguridad del art. 12 bis. y las responsabilidades por contenidos a las que hacen referencia los arts. 14 a 17 de la LSSI[24]. Además, cuando estos proveedores realicen operaciones de comercio electrónico, deberán cumplir con las obligaciones que exige la misma ley en relación al envío de comunicaciones electrónicas (arts. 19 a 22); al inicio de la contratación (art. 27); y a

21 En principio, las redes sociales y servicios *cloud* de software gratuitos pueden parecer poco rentables para el proveedor. Sin embargo, estas plataformas permiten reforzar marcas comerciales (el llamado *branding*) e impulsar la venta y/o descarga de determinados productos comerciales, facilitando el marketing viral. Existen estudios que demuestran que la atención a la publicidad en las principales redes es más alta (61%) que la prestada a los sitios web, (47%) y a *webmails* o blogs (38%). Fuente: PWC ESPAÑA, *EnREDados: Cómo hacer rentables las redes sociales* [en línea], 2012. Disponible en: <http://www.pwc.es/es_ES/es/publicaciones/retail-y-consumo/assets/enredados-como-hacer-rentables-las-redes-sociales.pdf> [Fecha de consulta: 19 de abril de 2017]. *Facebook*, la red social más extendida, con 1790 millones de usuarios activos en noviembre de 2016 y una media de 1.180 millones de usuarios activos diarios, se anotó un beneficio neto de 5.944 millones de dólares en los primeros 9 meses del mismo año. Fuente: SÁNCHEZ, J. M.; "No hay techo para *Facebook*: roza los 2.000 millones de usuarios" [en línea], *ABC Tecnología,* 2016. Disponible en: <http://www.abc.es/tecnologia/redes/abci-facebook-no-techo-para-facebook-roza-2000-millones-usuarios-201611031052_noticia.html>. [Fecha de consulta: 19 de abril de 2017].

22 El Tribunal de Justicia de la Unión Europea en la Sentencia de su Sala 3ª, de 15 de septiembre de 2016, C-484/2014, resuelve una cuestión prejudicial al respecto, e interpreta el concepto de "servicios de la sociedad de la información" de la Directiva 2000/31 del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico del mercado interior. En particular, establece que una prestación consistente en poner una red de comunicaciones a disposición del público de manera gratuita con fines publicitarios constituye un servicio de la sociedad de la información, en el sentido de la disposición anteriormente citada. Respecto de la onerosidad de los servicios de computación en la nube prestados sin que medie contraprestación dineraria por parte del usuario, véase apartado "Características de los contratos de servicios de computación en la nube: Contrato oneroso", en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

23 Ver capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

24 Ver capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

la confirmación del consentimiento y su aceptación (art. 28).

Para analizar esta cuestión, acudiremos otra vez a la Exposición de Motivos de la LSSI, donde enumera con una lista abierta los servicios de la sociedad de la información que se consideran actividades de intermediación: a) la provisión de acceso a la red; b) la transmisión de datos por redes de telecomunicaciones; c) la realización de copia temporal de páginas de Internet solicitadas por los usuarios; d) el alojamiento de información, servicios o aplicaciones en servidores; e) la provisión de instrumentos de búsqueda o enlaces a otros sitios de Internet; y f) cualquier otro servicio que se preste a petición individual de usuarios (descarga de archivos, etc.), siempre que represente una actividad económica para el prestador.

Continúa la Exposición de Motivos diciendo que "estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico".

La definición de servicio de intermediación recogida en su Anexo es la que sigue: "servicio de la sociedad de la información por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información".

A la vista de los contenidos expuestos, dependiendo de cuáles sean los servicios prestados y las capacidades informáticas suministradas por el proveedor de *Cloud Computing,* pueden encajar en las actividades, consideradas de intermediación por la LSSI, consistentes en la "transmisión de datos por redes de telecomunicaciones" (por ejemplo, correo electrónico, servicios que permiten compartir datos entre usuarios, etc.) o de "alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por terceros" (por ejemplo, servicios que impliquen el alojamiento remoto de información del cliente). Además, respecto de la actividad de intermediación consistente en alojamiento de información, consideramos que puede interpretarse extensivamente el término "servidores" como "centros de procesamiento y almacenamiento de datos". Cabe decir que, en la práctica, los proveedores *cloud* no se limitan a prestar uno de estos servicios de la sociedad de la información, sino varios, incluido el comercio electrónico.

En conclusión, bajo nuestro punto de vista un proveedor de servicios de computación en la nube podrá ser considerado un proveedor de servicios de intermediación a efectos de la LSSI, puesto que el objeto principal de los servicios de computación en la nube es la prestación de capacidades computacionales (procesamiento, almacenaje, etc.) que se transmiten mediante redes de

telecomunicaciones (en general, Internet), y que se encuentran automatizadas en centros de datos propiedad del proveedor, con independencia de que sea el usuario quien, una vez puestas a su disposición tales capacidades, las gestione a modo de autoservicio. La consecuencia legal para el proveedor será la obligación de someterse a las obligaciones que la Ley de Servicios de la Sociedad de la Información impone a los prestadores de servicios de intermediación, en especial el deber de colaboración del art. 11, el deber de información sobre medidas de seguridad del art. 12 bis, y las responsabilidades por contenidos de los arts. 14 a 17. A estos deberes y obligaciones nos referiremos en capítulos posteriores.

2.2.- El establecimiento del proveedor de servicios *cloud*

Determinada la condición de prestador de servicios de la LSSI, hemos de verificar cuando se aplicará esta norma española. En su Exposición de Motivos, resume que "desde un punto de vista subjetivo, la Ley se aplica, con carácter general, a los prestadores de servicios establecidos en España". Así lo establece también en su art. 2.1.

En cuanto a qué puede considerarse establecimiento en España, la Exposición de Motivos determina: "por «establecimiento» se entiende el lugar desde el que se dirige y gestiona una actividad económica (...)", y añade el segundo párrafo del artículo 2.1 que "se entenderá que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que estos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección". A tenor de este artículo, parece indiferente que el proveedor *cloud* tenga en España uno o varios centros de procesamiento de datos, si la efectiva gestión de este hardware se realiza en una sede sita en otro país diferente, por ejemplo Estados Unidos[25]. Y a la inversa, al proveedor le será plenamente aplicable la LSSI si la efectiva dirección del negocio *cloud* se desarrolla en sede española, aunque no radique en nuestro territorio ninguno de los centros de datos que utilice para prestar sus servicios.

Continúa la Exposición de Motivos: "La Ley resulta igualmente aplicable a quienes sin ser residentes en España prestan servicios de la sociedad de la información a través de un «establecimiento permanente» situado en España. En este último caso, la sujeción a la Ley es únicamente parcial, respecto a aquellos servicios que se presten desde España.(...)". Y añade el segundo párrafo del artículo 2.2: "se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que

25 No obstante, debe matizarse esta interpretación con los apartados 2 y 3 del mismo artículo, como veremos en los párrafos posteriores.

realice toda o parte de su actividad". Además, como aclara el último párrafo del art. 2.3, "la utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por si solo, el establecimiento en España del prestador".

Según el artículo 2.3, y en conexión con lo que hemos afirmado en el párrafo anterior, no es suficiente la existencia de un centro de datos en España para considerarse "establecimiento permanente". A la vista está, pues, que no puede considerarse un establecimiento permanente aquel centro de datos totalmente automatizado, situado en España, cuando todas las operaciones que procesa se ordenan desde una sede extranjera. Sin embargo, según lo dispuesto, ¿qué sucede si existe personal en España a cargo de su mantenimiento o de su gestión o administración? Según el art. 2.2, nos encontraríamos ante un "establecimiento permanente", porque ya existirán "lugares de trabajo" en territorio español donde se realiza parte de la actividad. Deberá diferenciarse, en este caso, si esa "actividad" es suficientemente relevante en relación a la actividad principal de la empresa para considerarla establecida permanentemente en España.

Sin embargo, la página web ministerial sobre una adecuada interpretación práctica de la LSSI reitera que "la utilización de un servidor situado en otro país no será motivo suficiente para descartar la sujeción a la Ley del prestador de servicios. Si las decisiones empresariales sobre el contenido o servicios ofrecidos a través de ese servidor se toman en territorio español, el prestador se reputará establecido en España"[26]. Si asimilamos el término "servidor" al término "centro de procesamiento de datos" (un centro de datos contiene múltiples equipos informáticos, entre ellos servidores), *a sensu contrario* será necesario que las decisiones que incumban al centro de datos español se tomen desde España para considerar al prestador de servicios como establecido permanentemente en nuestro país.

En cuanto a los prestadores de servicios situados en un Estado Miembro de la Unión Europea o del Espacio Económico Europeo, el art. 3.1 de la LSSI establece que: "sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes: a) Derechos de propiedad intelectual o industrial; (...) d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores; e) Régimen de elección por las partes contratantes de la legislación aplicable a su contrato; f) Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas".

26 Web oficial creada por el Ministerio de Industria y Turismo, en respuesta a la pregunta "¿Quiénes están sujetos a la Ley?". Disponible en: <http://www.lssi.gob.es/la-ley/Paginas/preguntas-frecuentes.aspx>. [Fecha de consulta: 19 de abril de 2017].

Es decir, en cuanto los servicios de computación en la nube afecten a estas materias, se aplicará la legislación española por ser la del destinatario residente o establecido en España, a no ser que las normas reguladoras de estas materias remitan el fuero a lugar distinto al de residencia o establecimiento del destinatario[27].

En relación a prestadores establecidos en países no miembros de la Unión Europea, determina el art. 4 de la LSSI que "les será de aplicación lo dispuesto en los artículos 7.2 y 11.2", con lo cual remiten a los acuerdos internacionales que resulten de aplicación (art. 7.2 LSSI) y a las decisiones de los órganos competentes en cuanto a la suspensión de un servicio de intermediación (art. 11.2 LSSI).

En resumen, quedan sujetos a la LSSI: a) los prestadores de servicios de sociedad de la información establecidos o residentes en España; b) los servicios prestados por prestadores de servicios de la sociedad de la información cuyas decisiones empresariales se adopten desde España, independientemente del lugar donde radiquen los centros de procesamiento de datos (asimilados al concepto de "servidores" recogido por la LSSI); c) los prestadores de servicios residentes o establecidos en un Estado Miembro de la Unión Europea o del Espacio Económico Europeo, atendiendo a las materias recogidas en el art. 3.1 LSSI, a la libre prestación de servicios y a sus restricciones (art. 7.1 LSSI), y al procedimiento de cooperación intracomunitario de los prestadores intermediarios (art. 8 LSSI); y d) los prestadores de servicios residentes o establecidos en terceros países, cuando dirijan sus actividades específicamente al territorio español, atendiendo a lo establecido en los acuerdos internacionales y a las restricciones a la prestación de servicios que atenten contra los principios del art. 8.1. LSSI.

---

27 En la contratación con consumidores, el fuero será el del domicilio de residencia del consumidor, atendiendo a lo establecido imperativamente por el art. 52.2 de la Ley de Enjuiciamiento Civil. El Auto del Tribunal Supremo (sala de lo civil, sección 1ª), de 20 de abril de 2009, declaró la competencia territorial al juzgado del lugar del domicilio de los consumidores, en un contrato de adhesión de servicios de transporte aéreo de pasajeros. La parte demandante era el consumidor (adherente) y la parte demandada, la compañía aérea. Como el contrato se celebró a través de Internet, las ciudades de residencia (y sede) de las partes no coincidían. La sentencia concluyó que debía ser en Palma de Mallorca, en virtud del fuero imperativo de competencia territorial (artículo 52.2 de la Ley de Enjuiciamiento Civil), especial para la protección de consumidores, cuya finalidad es facilitarles el proceso. En los contratos de consumo es habitual que las cantidades reclamadas no sean muy elevadas, con lo cual, si se obligase al consumidor a litigar en un fuero lejano, se perjudicaría gravemente su derecho a la tutela judicial efectiva. Recuerda también la sentencia que la Ley de Consumidores y Usuarios estipula como cláusula abusiva el pacto de sumisión expresa que no sea a favor del lugar del domicilio del propio consumidor, a la vez que destaca la imperatividad de estas normas de protección de consumidores.

Como dice la propia Ley, el lugar de establecimiento del prestador de servicios es "un elemento esencial (...), porque de él depende el ámbito de aplicación no solo de esta Ley, sino de todas las demás disposiciones del ordenamiento español que les sean de aplicación, en función de la actividad que desarrollen. Asimismo, el lugar de establecimiento del prestador determina la ley y las autoridades competentes para el control de su cumplimiento, de acuerdo con el principio de la aplicación de la ley del país de origen que inspira la Directiva 2000/31/CE".

3.- EL SUSCRIPTOR DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

Como hemos podido observar, las ventajas de la computación remota pueden beneficiar a particulares y a entidades públicas y privadas. Sin embargo, tanto las eventuales negociaciones como las condiciones contractuales pueden ser diferentes dependiendo de quién sea el destinatario de los servicios[28].

A continuación, analizaremos las tres posibles condiciones de la parte contratante de servicios de computación en la nube: empresario, consumidor o Administración Pública, sin perjuicio de que, como hemos mencionado en distintas ocasiones, nos centremos en el estudio de las contrataciones efectuadas por el pequeño empresario que suscribe servicios de computación en la nube a través de condiciones generales predispuestas mediante contratación electrónica.

3.1.- El empresario como suscriptor. Breve referencia a sus empleados

Las empresas que demandan servicios de computación en la nube comprenden una diversidad que abarca desde grandes multinacionales con dispares objetos sociales (relacionados o no con el sector tecnológico) hasta pequeñas *start-ups*[29]. En este apartado, nos centraremos en la contratación de servicios de

28 Debemos distinguir entre el suscriptor de los servicios (es decir, quien manifiesta el consentimiento contractual y paga o no un precio por el servicio) del destinatario o usuario de los servicios, (aquel que utiliza los servicios *cloud*). De este modo, una empresa podrá ser suscriptora de servicios *cloud* y a su vez destinataria, si los integra en su proceso productivo, o no destinataria si los vende a sus propios clientes. A su vez, el consumidor será el suscriptor de aquellos servicios *cloud* que el mismo ha contratado; o usuario de servicios *cloud* suscritos por una empresa de la cual es cliente y como tal, tiene autorización para aprovechar sus funcionalidades (por ejemplo, los particulares usuarios de aplicaciones para dispositivos móviles cortesía de marcas comerciales, como la que ofrece la textil Mango). <http://www.goldengekko.com/?our_work_projects=mango-mng> y <http://shop.mango.com/iframe.faces?state=she_001_ES>. [Fecha de consulta: 2 de junio de 2017].

29 *Startups*: empresas de nueva creación, generalmente relacionadas con el sector TIC, con grandes posibilidades de crecimiento y tendencia a la escalabilidad. Además, suelen buscar sistemas de

computación en la nube por vía electrónica y cláusulas predispuestas por parte de pequeños empresarios y profesionales, sin perjuicio de que existan contratos negociados entre proveedores *cloud* y grandes empresas, que presentan algunas características diferentes.

3.1.1.- El empresario como destinatario y eventualmente, subproveedor de servicios de computación en la nube

Los motivos que pueden conducir a una empresa a utilizar soluciones de computación remota son tan diversos como pueden serlo sus operativas internas. Los servicios *cloud* pueden combinarse o superponerse de acuerdo con las capas arquitectónicas que los sostienen, y un mismo servicio puede compaginar componentes hardware y software de diferentes proveedores[30]. Del mismo modo, pueden suscribirse capacidades *cloud* de diferentes proveedores, por ejemplo, múltiples servicios de software *cloud* que den acceso al cliente a funcionalidades diferentes o complementarias. De ahí que las implicaciones legales de la contratación de servicios de computación en la nube alcancen, en ocasiones, altos grados de complejidad.

Ahora bien, como ya hemos mencionado, entre los suscriptores de servicios *cloud*, algunos integrarán simplemente las capacidades o servicios computacionales

---

financiación diferentes a los tradicionales, como el *Venture Capital* (porcentajes del accionariado de la empresa a cambio de aportaciones de capital realizadas por inversores). La gran mayoría de *start-ups* ofrece software como servicios, webs colaborativas o 2.0, o aplicaciones. (Definición propia). Como ejemplos de empresas que se iniciaron como *start-ups,* la madrileña Next Limit (que diseñó un software de simulación de fluidos y que ganó un óscar técnico en 2008 por los efectos especiales de la película "El Señor de los Anillos"), la valenciana Robotnik, (especializada en robótica, ha diseñado un brazo modular que sirve para desactivar explosivos o tomar muestras potencialmente contaminadas). Grandes empresas tecnológicas como Facebook, Twitter, Dropbox o Instagram también empezaron siendo *start-ups*. Muchas de ellas fundamentan actualmente su arquitectura interna en la nube, proveyéndose así de recursos de infraestructura o plataforma suficientes para sustentar las necesidades de computación de sus aplicaciones. Fuentes: PÉREZ, David; *Start-ups españolas que nacieron ayer y facturan millones* [en línea], 2013. Disponible en: <http://www.elconfidencial.com/multimedia/album/tecnologia/2013-08-30/startups-espanolas-que-nacieron-ayer-y-facturan-millones_22628/>. [Fecha de consulta: 19 de abril de 2017]. OTTO, Carlos; *Las start-ups españolas conquistan el mundo* [en línea], 2016. Disponible en: <http://www.lavanguardia.com/vangdata/20160616/402552055207/startup-espanolas-conquistan-el-mundo.html>. [Fecha de consulta: 19 de abril de 2017]. HOLIDAY, Ryan; *How Facebook, Twitter and Other Start-ups Got Big* [en línea], 2014. Disponible en: <http://www.huffingtonpost.com/ryan-holiday/how-facebook-twitter-and-_b_4228942.html> [Fecha de consulta: 19 de abril de 2017].

30 Ver apartado "Las capas que integran la nube y su tecnología subyacente", en el capítulo "Concepto y características técnicas de la computación en la nube".

suministrados en su propio proceso productivo, mientras que otros, cuya actividad económica sea la prestación de servicios relacionados con el sector TIC, se convertirán a su vez en suministradores de entornos más o menos integrales de *cloud computing* a sus propios clientes (infraestructura como servicio, plataforma como servicio, software como servicio o combinaciones de estos). En ocasiones, se sitúan en el último eslabón de cadenas de contratos de suministros que son totalmente desconocidas para el usuario final del servicio[31]. Es así que estas empresas ocuparán a la vez las posiciones jurídicas de proveedor y de usuario de servicios *cloud*, dentro de un conjunto de relaciones jurídicas que involucran no solo a otros proveedores y usuarios de la propia cadena, sino también a otros cousuarios de los mismos equipos físicos, a prestadores de servicios accesorios, a titulares de derechos de propiedad intelectual y a titulares de datos personales.

Tengamos en cuenta, en este sentido, que los usos de la computación en la nube son cada vez más sofisticados y que un usuario puede ocupar diferentes roles dentro de un mismo entorno, contratar en diferentes mercados con diferentes clientes e ir acumulando obligaciones legales y responsabilidades. Además, con tantos actores implicados en el marco jurídico actual, caracterizado por la falta de normativa específica y de precedentes jurisprudenciales, la determinación de tales responsabilidades puede ser problemática, especialmente en aquellos casos en los que no exista una clara delimitación de las obligaciones asumidas y de las actividades y funciones realizadas por cada uno de estos participantes dentro de un mismo entorno.

Para una exposición más clara, veamos las combinaciones de suministros que pueden tener lugar[32]:

a) La infraestructura como servicio (IaaS) puede levantarse sin necesidad de otro servicio *cloud* que lo sustente, sino que lo provea un propietario o inquilino de

31 Por ejemplo, los clientes de Dropbox pueden creer que el software cloud de almacenamiento que se les ofrece está basado en tecnología propiedad exclusiva de Dropbox. Sin embargo, Dropbox ha levantado su servicio sobre el servicio de infraestructura cloud que le suministra Amazon. Así, Amazon es el verdadero proveedor de infraestructura sobre el que se sustenta el software como servicio de Dropbox, y como tal le corresponde parte de la prestación del servicio, concretamente la relativa a los centros de datos físicos y las máquinas virtuales en las cuales se realiza el almacenamiento de información. Dropbox, por lo tanto, es a la vez usuario de servicios de infraestructura *cloud* y prestador de servicios de software *cloud*.

32 KUAN HON, W; MILLARD, C; "Cloud Technologies...", *op. cit.*, pág. 15.

uno o más centros de datos físicos adecuadamente equipados[33].

b) La plataforma como servicio (PaaS), al igual que sucede con la infraestructura como servicio, puede levantarse directamente desde la capa hardware[34] física o sobre otro servicio de infraestructura.[35]

c) El software como servicio (SaaS) puede levantarse de tres maneras: sin capa *cloud* inferior[36], directamente sobre un servicio de infraestructura (IaaS)[37] o sobre un servicio de plataforma (PaaS), el cual, como acabamos de mencionar, puede a su vez levantarse desde un servicio de infraestructura (IaaS)[38] o directamente desde un centro de procesamiento de datos[39].

Toda esta cadena de suministros puede verse en la siguiente figura de forma más ilustrativa[40].

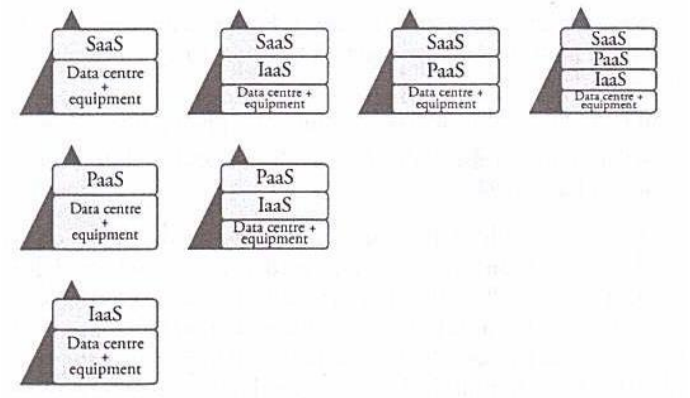

Figura nº 3. Cadena de suministros de servicios de computación en la nube.

Como se ha dicho, toda esta arquitectura aparece a menudo ante el usuario final como un único servicio *cloud*, y este puede depender, en realidad, de bastantes

33 Como *Amazon Web Services*, *Rackspace*, *GoGrid* o *Google Compute Engine*.

34 Por ejemplo, *Google App Engine*, *Windows Azure* de Microsoft o *Force.com* de *Salesforce.com.*

35 Como *dotCloud, Engine Yard* o *Heroku*, todas levantadas sobre la IaaS de *Amazon.*

36 Como muchas redes sociales (*Facebook* o *Flickr)* o servicios de correo electrónico (como *Gmail* u O*utlook.com*).

37 Como *Dropbox* o *Mozy*, ambas sobre IaaS de Amazon.

38 Por ejemplo, software como servicios levantados sobre servicios de plataforma (PaaS) que a su vez se sustentan el servicios de infraestructura (IaaS), al igual que los mencionados *dotCloud* o *Heroku*.

39 Por ejemplo, cualquier software como servicio levantado sobre *Google App Engine* o Microsoft *Azure.*

40 Figura nº 3. Fuente: KUAN HON, W; MILLARD, C; "Cloud Technologies...", *op. cit.*, pág. 15.

proveedores y subproveedores diferentes, entre los cuales mediarán sendos acuerdos contractuales. Y aunque es posible que un usuario particular contrate con un único proveedor integral de todo el entorno, en la mayoría de los casos los proveedores se autoabastecen entre sí de recursos para contar con el óptimo equipamiento para aprovisionar a sus propios clientes.

Cuando son varios los proveedores que integran una cadena de servicios a modo de subcontrata, entre ellos sería conveniente acordar la responsabilidad por la prestación del servicio al cliente, para lo cual deberán estar perfectamente delimitadas las funciones de cada uno de ellos con el fin de acotar eficazmente las responsabilidades que corresponden a cada uno. Sin embargo, aunque sería recomendable, esta no es una solución que se adopte de manera habitual por los proveedores. Siendo este apartado meramente descriptivo de la realidad de las partes contractuales, nos remitimos a capítulos posteriores para un análisis más detallado de la responsabilidad del proveedor sobre sus subcontratas[41].

3.1.2.- El rol del CTO como responsable técnico de la empresa

Dentro de este complejo entramado de servicios informáticos tiene especial importancia el llamado CTO, acrónimo del término inglés *Chief Technology Officer,* o director de tecnología, quien aunque no ocupe la posición jurídica de parte contractual, juega un papel relevante en la contratación al ser la persona física que ocupa el máximo cargo dentro del departamento tecnológico en la empresa cliente, y que es el responsable técnico de la gerencia e implementación de las tecnologías de la información[42]. Si bien, como hemos apuntado, este trabajo se centra en contratos suscritos por pequeños empresarios, y aunque no sea un cargo habitual en la pequeña empresa y microempresa, queremos hacer referencia a esta figura puesto que, en algunas empresas medianas es habitual que un empleado actúe a modo de responsable del departamento informático o dirija las operaciones tecnológicas de la empresa, razón por la cual consideramos conveniente describir sus funciones

41 Para un estudio más detallado de la responsabilidad de los subproveedores, nos remitimos al apartado "La responsabilidad del proveedor por actuaciones de los subproveedores", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

42 También es común el acrónimo CIO (del inglés *Chief Information Officer*), aunque en definitiva se trata de la persona física responsable de desarrollar la visión tecnológica del negocio empresarial, quien a menudo ocupa una posición ejecutiva dentro del Departamento de Tecnología de la Información (u homólogo).

principales dentro de la empresa suscriptora de servicios *cloud*[43].

El CTO o director de tecnología, encargado de solventar las necesidades tecnológicas para que la empresa pueda desarrollar su objeto social, puede tener diferentes nombres dentro del organigrama empresarial, aunque presentará ciertas características comunes:

a) tiene conocimiento de las necesidades informáticas de la empresa y del presupuesto disponible para cubrir tales necesidades;

b) tiene conocimientos suficientes para entender e informar sobre la implementación de una estrategia capaz de cubrir estas necesidades; y

c) es consciente de los beneficios y riesgos que puede suponer para la empresa la adopción de cambios tecnológicos (entre ellos, la implementación de un entorno de computación en la nube): seguridad de los datos, fiabilidad del sistema, disponibilidad del servicio, portabilidad, etc.

Independientemente de que sea el propio CTO quien suscriba o no, como representante de la empresa, un contrato de suministro de computación remota, no dejan de ser relevantes las responsabilidades que conlleva el desempeño de su cargo dentro del proceso de negociación, contratación, prestación y terminación del servicio para su empresa[44]. Los conocimientos técnicos que posee fruto de su formación, experiencia, y de la colaboración con el equipo de profesionales que eventualmente dirija, lo sitúan como figura clave para determinar aspectos tan importantes como:

1) la elección más acertada de proveedor, una vez estudiados no solo los costes económicos, sino otros detalles esenciales para la operativa empresarial, como la capacidad de negociación o no de ciertas cláusulas individuales; la necesidad de rediseñar procesos, sistemas y aplicaciones que tiene la empresa en sus activos para poder implementar un modelo público, privado o híbrido; la accesibilidad y control de los datos por parte de la empresa y la cesión de control al proveedor; la garantía ofrecida por sus sistemas y equipos; la custodia de la información empresarial almacenada por el proveedor, etc.

43 No todas las empresas tendrán una figura en su organigrama interno que represente al CTO, sino que sus funciones pueden encontrarse diluidas entre diversos actores o contratadas externamente, o simplemente asumidas por el propio pequeño empresario.

44 Siempre y cuando posea las potestades legales que le facultan para obligar a la empresa con un contrato de suministro de computación remota.

2) la elección más adecuada del servicio o conjunto de soluciones, para que proporcione una reducción de costes y mejore la eficiencia de los recursos hardware y software disponibles en la empresa, haciéndola más competitiva;

3) la veracidad y transparencia de la información aportada al proveedor y de la facilitada por este

4) la comprensión del acuerdo de nivel de servicio y de otros anexos y requisitos técnicos que se recojan en el contrato;

5) la calidad del suministro efectivamente prestado y su adecuación a lo contratado;

6) la elaboración de planes de emergencia en caso de fallos o caídas del sistema, o de pérdida de datos, en colaboración o no con el proveedor elegido; el tanteo de proveedores alternativos de servicios; y el procedimiento de recuperación de datos una vez finalizado el servicio, puesto que la imposibilidad por parte de la empresa del acceso a sus datos puede implicar graves pérdidas económicas, desprestigio empresarial, perjuicios para los usuarios finales[45] y, consecuentemente, pérdida de posición en el mercado de la empresa[46].

Además, es aconsejable su colaboración con el departamento legal, para asegurar el cumplimiento, entre otras regulaciones, de la normativa técnica y de seguridad específica que rija el sector al cual pertenece la empresa, y de la legislación de protección de datos personales.

En definitiva, un cumplimiento diligente del CTO puede minimizar futuros conflictos entre la empresa y su proveedor de servicios de computación en la nube. En cambio, su negligencia o falta de pericia puede generar responsabilidades para la empresa ante el proveedor o ante terceros.

3.1.3.- Los empleados y clientes del empresario suscriptor

Pese a no haber suscrito por ellos mismos ningún contrato de suministro *cloud*, los empleados de la empresa son quienes dan uso al hardware y software que esta pone a su disposición para que lleven a cabo determinadas funciones, ya sea

45 Pongamos por ejemplo los daños causados por caídas de sistema a los clientes de una entidad bancaria o a los usuarios de un servicio sanitario.

46 Por ejemplo, la caída de una web de contratación turística o de compras en línea en fechas clave para la campaña de Navidad.

como usuarios de hardware virtualizado mediante servicios *cloud* de infraestructura (IaaS), como desarrolladores de software con plataformas como servicio (PaaS) o de aplicaciones de software como servicio (SaaS) de gestión de diferente operativa empresarial o estrategia comercial[47].

Por otra parte, el proveedor a menudo pone a disposición de la empresa cliente mecanismos destinados a monitorizar los usos del servicio por parte de sus empleados[48]. La información extraída puede fundamentar decisiones relacionadas con la gestión de recursos económicos y humanos de cada uno de los departamentos, el cumplimiento de objetivos empresariales y control de acceso y uso de cierta información empresarial delicada.

Los empleados deben hacer un uso responsable y lícito de las herramientas que se les facilitan, sobre todo en relación al cumplimiento de las políticas de uso adecuado PUA contratadas entre proveedor *cloud* y empresa[49]. Así, es recomendable

47 A modo de ejemplo, la empresa hostelera The Eat Out Group, representante de marcas como *Burguer King, Bocatta o Pans & Company,* migró en 2014 la gestión de recursos humanos, áreas de personal y nóminas a la nube, de la mano de *SAP España* y su servicio software "*Success Factors EC Payroll"*. Esta aplicación permite a los empleados acceder al portal y consultar sus datos profesionales y saber quiénes son los miembros de su equipo. Además, pueden realizar determinadas gestiones en línea, como pedir anticipos o generar altas y bajas. Toda esta información está centralizada a través de un único punto de acceso, evitando doble "input" de trabajadores y facilitando la monitorización de accesos y modificaciones de datos. Como resultado, ha conseguido reducir en un 30% el coste costes de gestión de personal y nómina, en su empresa de más de 1700 empleados. Fuente *The Eat Out Group traslada a la nube la gestión de recursos humanos y nómina de la mano de SAP, [en línea]*: <http://www.revistacloudcomputing.com/2014/11/the-eat-out-group-traslada-a-la-nube-la-gestion-de-rrhh-y-nomina-de-la-mano-de-sap/>. [Fecha de consulta: 28 de julio de 2016].

48 Nos referimos a la monitorización de accesos, modificaciones y retiradas de datos empresariales almacenados en la nube, es decir, de actividades que el empleado realiza con las herramientas *cloud* suministradas por la empresa, que pueden colisionar con el derecho a la intimidad del trabajador. Por otra parte, la monitorización, puede servir a la empresa para determinar la productividad de un concreto empleado o investigar presuntas violaciones de políticas de uso adecuado (PUA). Respecto del servicio de correo electrónico, cabe mencionar la sentencia del Tribunal Constitucional del 7 de octubre de 2013, de la que se deduce que, al establecerse expresamente por la empresa una política de uso limitado a finalidades exclusivamente profesionales de las herramientas informáticas que cede al trabajador, el ejercicio de su potestad de vigilancia no se verá impedido por mera colisión con los fundamentales derechos a la intimidad y al secreto de las comunicaciones. Esta potestad, que no otorga en manera alguna patente de corso al empresario, viene conferida por el art. 20.3 del Estatuto del Trabajador, y debe ejercerse con las oportunas garantías.

49 Política de Uso Adecuado (PUA). Cláusula o conjunto de cláusulas que regulan la manera en la que los clientes deben utilizar el servicio *cloud*, e incluyen determinadas acciones prohibidas. (Definición propia). Ver apartado "Legalidad y adecuación de los contenidos alojados por el

que el departamento responsable de recursos humanos (u otro, según determine el organigrama empresarial) les informe de la existencia de ciertas actividades prohibidas por inadecuadas, impropias o dañinas, al usar las herramientas *cloud*. Estas pautas y restricciones información puede incorporarse análogamente a modo de cláusula o anexo en los contratos de trabajo que se suscriban una vez implementada la nube en la empresa.

No olvidemos, igualmente, la importancia de la formación al trabajador en aspectos esenciales de la normativa sobre protección de datos personales y de su cumplimiento adaptado a la nube, así como de la confidencialidad de los datos y secretos empresariales. Al mismo tiempo, sería interesante informarles de la existencia de derechos de propiedad intelectual titularidad de la empresa, del proveedor o de terceros propietarios de software, para evitar posibles responsabilidades devengadas por desconocimiento.

Finalmente, los clientes de las empresas suscriptoras también pueden verse beneficiados por las ventajas de la computación en la nube. Es común que, a través de aplicaciones, se les permita acceder a contenidos específicos mediante claves de identificación personal, y realizar determinadas acciones en línea, por ejemplo editar sus datos de cliente, efectuar pedidos, consultas, compras electrónicas u otros trámites en línea con la empresa[50]. Para estas tareas, es habitual que, en cumplimiento de la legislación sobre protección de datos, deban acceder a la cesión de sus datos personales y se les informe del tratamiento que se dará a tales datos[51]. Sin embargo, a nuestro parecer los clientes que sean usuarios del servicio también deberían suscribir, o al menos ser informados, sobre los usos prohibidos del servicio (es decir, de una política de uso adecuado o PUA[52]) y de la información sobre eventuales monitorizaciones que puedan tener lugar durante el uso que realicen del servicio.

---

usuario. las políticas de uso adecuado PUA) y su control por el prestador de servicios", en el capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

50 Por ejemplo, consultar datos de nuestros envíos a través de la empresa de transportes Seur (gracias al sistema *cloud* proporcionado por el proveedor HP), o realizar transferencias electrónicas de dinero como usuarios de banca electrónica.

51 Ver capítulo "Privacidad en la nube. Principales cuestiones sobre protección de datos de carácter personal".

52 Ver apartado "Legalidad y adecuación de los contenidos alojados por el usuario. Las políticas de uso adecuado y su control por el prestador de servicios", en el capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

3.2.- El consumidor de servicios de computación en la nube

Hemos mencionado en diversas ocasiones que la contratación de servicios *cloud* tiene lugar mayoritariamente en línea, y que es susceptible de suscribirse por un conjunto heterogéneo de suscriptores que abarca empresas de diferentes dimensiones, profesionales independientes, consumidores y Administraciones Públicas.

En el supuesto de contratación electrónica de los servicios y bajo condiciones de adhesión por parte de consumidores, durante la fase previa a la contratación que tiene lugar en el sitio web del proveedor, se suele ofrecer la misma plataforma electrónica para acceder a las características de todos los servicios *cloud* que se ofertan, y a las condiciones contractuales. Con carácter general, el formulario de registro se cumplimenta mediante la selección de opciones y la introducción de caracteres en casilleros, lo cual permite al cliente, en muchas ocasiones, identificarse como consumidor, representante de persona jurídica o profesional independiente[53]. Sin embargo, en otras ocasiones es el propio producto el que se dirige a cubrir las necesidades de un sector específico, con lo cual el cliente interesado podrá decantarse por uno u otro servicio según el uso profesional o personal que pretenda conferirle[54]. Resulta evidente que, en aquellas situaciones en las que el cliente, al rellenar el formulario electrónico de contratación, se registra inicialmente como profesional o representante de una empresa, y como tal contrata el servicio *cloud*, quedaría en principio sujeto a las cláusulas suscritas en ese contrato destinado al público profesional, aunque decidiera dedicar el servicio a finalidades exclusivamente personales.

En aquellos casos en los que el cliente se identifique ante el proveedor como particular, puede ocurrir que contrate inicialmente con propósitos personales pero, posteriormente, decida ampliar el uso del servicio a tareas relacionadas con su

53 En la mayoría de los contratos de suscripción de servicios de computación en la nube en línea mediante condiciones generales, nos encontramos con una cláusula que establece que es responsabilidad del cliente la veracidad de los datos facilitados, así como la reserva del derecho a denegar la contratación a discreción del proveedor. Así aparece en las condiciones generales ofrecidas en su sitio web por los proveedores *Accens* y *Box*. <http://www.acens.com/corporativo/politicas-y-condiciones-de-uso/> y <https://www.box.com/legal/termsofservice/ES/> [Fecha de consulta: 19 de abril de 2017].

54 Salesforce oferta en su web "soluciones para pequeñas empresas". Facebook ofrece "perfiles" a sus usuarios particulares y "páginas" a entidades, marcas o figuras públicas, unos y otras con diferentes condiciones.

negocio. Por otro lado, la propia naturaleza de las capacidades computacionales implica que estas sirvan tanto a propósitos empresariales o profesionales como personales, en ciertos casos difícilmente diferenciables. Esta cualidad es predicable principalmente de los servicios *cloud* de software (SaaS) que cubren necesidades estándares y no personalizadas[55].

Lo dicho hasta aquí pone de manifiesto la dificultad de determinar, en la contratación de servicios de computación en la nube, cuándo el contratante se considera consumidor protegido a efectos del Real Decreto Legislativo 1/2007, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (en adelante, TRDCU), de la Ley 34/2002 de Servicios de la Sociedad de la Información, y de demás regulación concerniente a la protección de consumidores; y cuándo queda fuera de esta regulación.

Como veremos a continuación, los clientes pueden dar usos mixtos a los servicios de computación en la nube. La importancia de determinar el uso particular o profesional al cual el cliente dedica el servicio radica en la aplicación, en caso de usos no profesionales, de la mencionada normativa de protección al consumidor. Al menos en principio, parece ser que no podrán beneficiarse de esta tutela los usuarios que dediquen el servicio mayormente a actividades empresariales o profesionales, al igual que sucederá con los contratantes que sean pequeños empresarios[56].

3.2.1.-El concepto legal de consumidor y la eventual dificultad de la delimitación de los usos profesionales y particulares del servicio *cloud*

Con la reforma del TRDCU introducida por la Ley 3/2014, que transpone al derecho interno la Directiva 2011/83/CE, se modifica el concepto de consumidor y

55 Por ejemplo, un servicio de almacenamiento de datos en la nube, o de correo electrónico.

56 Coincidiendo con la opinión de otros autores (entre otros, MIRANDA SERRANO, Luís; PAGADOR LÓPEZ, Javier; "Bienvenidas sean recientes decisiones judiciales favorables a someter a control de contenido las condiciones generales utilizadas frente a adherentes empresarios o profesionales [en línea]. Disponible en: <http://www.ccopyme.org/articulo.php?a=84>. [Fecha de consulta: 17 de enero de 2017]), y como argumentaremos en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube", abogamos por una aplicación extensiva de las cláusulas abusivas destinadas a proteger al consumidor en aquello casos en los que el pequeño empresario suscriptor de servicios *cloud* se encuentre en una situación de indefensión similar, debido al desconocimiento de la técnica involucrada y al desequilibrio económico y de poder como parte contractual débil.

usuario. Con esta reforma, el art. 3 del TRDCU define así este término: "A efectos de esta norma y sin perjuicio de lo dispuesto expresamente en sus libros tercero y cuarto, son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión. 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".

Por su parte, el Anexo de la Ley 34/2002 de Servicios de la Sociedad de la Información remite al concepto de consumidor del art. 1 de la Ley 26/1984 General para la Defensa de Consumidores y Usuarios. Este ha sido derogado por el posterior TRDCU y reformado por la Ley 3/2014, con lo cual se refiere al concepto mencionado en el párrafo anterior (art. 3 TRDCU).

De acuerdo con lo expuesto anteriormente, cuando los recursos *cloud* se utilicen claramente para fines comerciales, empresariales o profesionales, en principio quedarán excluidos del amparo de la legislación de protección al consumidor. Así sucederá cuando el suscriptor de los servicios sea una empresa o un profesional[57]. Por contra, cuando estos recursos atiendan únicamente a propósitos personales, será aplicable la normativa mencionada[58].

Sin embargo, algunos servicios *cloud* de software [59] (como servicios de correo electrónico o software de procesamiento de textos) son susceptibles de generar usos mixtos, lo cual no sucede con otros servicios (como el software enfocado especialmente a usos empresariales, como puede ser una aplicación de gestión de recursos humanos o de datos de clientes). Por ello, será importante la declaración que realice el suscriptor en el momento de la contratación del servicio *cloud*, en atención a si la persona física se identifica como particular o como profesional. Cuando lo declarado no coincida con el verdadero uso dado al servicio, el juzgador

57 Dedicamos un apartado específicamente a empresarios adherentes en contratos predispuestos de servicios de computación en la nube, titulado "Breve reflexión relativa a la aplicación extensiva de las normas y criterios sobre cláusulas abusivas al pequeño empresario", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

58 En la sentencia de la Audiencia Provincial de Toledo, sección primera, de 16 de marzo de 2000, el tribunal falla que "es claro que habrán de quedar excluidos del concepto de consumidores y usuarios los adquirentes de los bienes o servicios que los emplearan o integraran en un proceso empresarial, comercial o profesional, en lugar de ser meros destinatarios o usuarios finales de los mismos, lo que evidentemente concurre en el caso de autos,(...)", criterio compartido, junto a otros afines de diferentes sentencias, por el Fundamento Jurídico 2º de la Sentencia de la Audiencia Provincial de Valencia de 10 de marzo de 2001, en el que se establece la relevancia de la finalidad del programa informático que se introdujo en la cadena de producción para el control de ventas.

59 Los servicios *cloud* de infraestructura (IaaS) y plataforma (PaaS) están enfocados a su uso por empresas y profesionales de la informática. Sin embargo, nada obsta a que pueda contratarlos un particular.

deberá determinar el uso predominante que el suscriptor da al servicio una vez contratado[60]. Si ese uso es esencialmente personal, existen mayores argumentos a favor de que esa persona física sea considerada consumidor, y, por tanto, beneficiario de la protección de la normativa[61].

Cuando el contratante no tenga la condición de consumidor de acuerdo con la definición legal, las normas destinadas a paliar el desequilibrio entre las partes contractuales en materia de consumo no le resultan, en principio, aplicables, y este contratante no se puede acoger, por lo general, a la protección del consumidor. En otras palabras, el contratante carecerá del amparo de las normas imperativas y de las presunciones que protegen al consumidor, y no le será aplicable, en principio, la nulidad de las eventuales cláusulas abusivas que hubiera podido suscribir[62].

---

60 Por ejemplo, si el juzgador atiende al uso que se realiza del servicio, en el caso de que el usuario contratara un servicio de almacenamiento de datos en la nube, si los datos migrados son en su mayoría personales (fotos, vídeos familiares, etc.), será susceptible de ser considerado consumidor. En cambio, si el espacio está ocupado sobre todo por archivos relacionados con el negocio, será considerado profesional y, por tanto, puede quedar excluido de la tutela dedicada al consumidor.

61 Según la legislación anglosajona de contratación al consumidor contenida en la *Unfair Contract Terms Act*, de 1977, en su sección 12, un cliente contrata como consumidor si se cumplen tres requisitos: el primero es que no suscriba el contrato dentro del curso de una actividad empresarial ni tenga intención de hacerlo; en segundo lugar, que la otra parte ofrezca el contrato en el curso de una actividad comercial; y por último, que el tipo de bienes adquiridos pertenezcan a la categoría de bienes que los consumidores suelen adquirir (traducción propia del original en inglés: "A party to a contract "deals as consumer" in relation to another party if: a) he neither makes the contract in the course of a business nor holds himself out as doing so; and b) the other party does make the contract in the course of a business; and c) in the case of a contract governed by the law of sale of goods or hire-purchase, or by section 7 of this Act, the goods passing under or in pursuance of the contract are of a type ordinarily supplied for private use or consumption"). Puesto en relación con el *cloud computing*, lo relevante para el legislador británico es la intención del consumidor en el momento de suscribir el contrato, es decir, que el usuario al contratar pretenda destinar el servicio a usos particulares en el momento de suscribir el contrato. La Directiva 93/13/CEE sobre cláusulas abusivas en contratos con consumidores no es tan explícita, al definir al consumidor en su art. 2 como "toda persona física que, en los contratos regulados por la presente Directiva, actúe con un propósito ajeno a su actividad profesional". Sin embargo, consideramos que la reforma introducida por la Ley 3/2014 en el TRDCU abarca también la actividad posterior al momento de perfección del contrato, es decir, el uso efectivo que se da al servicio, al centrarse el art. 3 en la actuación del consumidor: "A efectos de esta norma (...), son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión. 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".

62 El juzgador podría aplicar de manera analógica la normativa de protección al consumidor, al valorar que el adherente pequeño empresario se encuentra en una situación de desprotección equiparable a la del consumidor. Ver apartado "Breve reflexión relativa a la aplicación extensiva de las normas y criterios sobre cláusulas abusivas al pequeño empresario", en el capítulo

A continuación, exponemos las principales normas de protección al consumidor y su relación con la suscripción *online* de servicios de *Cloud Computing,* puesto que en este trabajo, como veremos en capítulos posteriores, se plantea la tesis de la aplicación extensiva de protección del consumidor al pequeño empresario que presenta una situación de indefensión equiparable a la del consumidor cuando contrata servicios de computación en la nube.

3.2.2.- La protección del consumidor y su incidencia en la contratación de servicios de computación en la nube

La concreta protección del consumidor se materializa, por una parte, mediante actuaciones preventivas que pretenden evitar lesionar los intereses del consumidor y, por otra parte, a través de otras actuaciones posteriores a la suscripción del contrato. Y aunque en este apartado no pretendemos efectuar una recopilación exhaustiva, sí recogeremos las más relevantes para los consumidores de servicios *cloud,* sin perjuicio de que la aplicación de algunas de estas normas sea igualmente procedente (en inicio o a partir de una aplicación analógica) a la contratación de servicios *cloud* por profesionales.

En primer lugar, los métodos de protección preventiva del consumidor abarcan ciertas prohibiciones para los proveedores y el cumplimiento de otras tantas obligaciones en diferentes cuestiones, en especial:

a) la identificación de prácticas comerciales desleales de las empresas en sus relaciones con el consumidor reguladas por la Directiva 2005/29/CE sobre prácticas comerciales desleales y su transposición a la normativa española mediante la Ley 29/2009 de 30 de diciembre. Esta Ley, aplicable a contratos suscritos tanto por consumidores como por empresas, modificó concretamente la Ley 3/1991 de Competencia Desleal, la Ley 7/1996 de Ordenación del Comercio Minorista, la Ley 34/1998 General de Publicidad y el TRDCU. Como ejemplos de tales prácticas comerciales abusivas, podemos referir: la exhibición de sellos de confianza o de calidad sin haber obtenido la necesaria autorización[63] (art. 21 de la Ley 3/1991 de

"Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

63 En el ámbito de servicios en la nube, sirva como muestra la certificación *EuroCloud Star Audit* (ECSA), avalada e impulsada por la Unión Europea, que garantiza un alto nivel de seguridad de los servicios *cloud*. <https://eurocloud-staraudit.eu/>. [Fecha de consulta: 20 de abril de 2017]. En EEUU tuvo lugar un caso de engaño sobre certificaciones de seguridad, aunque no frente a

Competencia Desleal); el error en cuanto a las características, composición y riesgos del servicio y el alcance de los compromisos del empresario o profesional[64] (arts. 5.1.b y 5.d respectivamente, de la misma Ley 3/1991) o la omisión de la información necesaria para que el destinatario pueda adoptar una decisión con el debido conocimiento de causa (art. 7 de la Ley de Competencia Desleal);

b) la regulación en materia publicitaria, recopilada en la Ley 34/1998 General de Publicidad y en el TRDCU. Entre otras acciones, recoge en su artículo 3.b la publicidad que incite a menores a la suscripción de un servicio, aprovechándose de su inexperiencia o credulidad.[65]

c) la regulación de la venta a distancia y del comercio electrónico[66], amparada por las Directivas 97/7/CE y 2000/31/CE. En España esta regulación se recoge en las Leyes 47/2002 de Ordenación del Comercio Minorista (en adelante, LOCM), el TRDCU y la LSSI, entre otras[67], y sus principales acciones son la obligación de facilitar al consumidor cierta información de forma clara y comprensible antes de suscribir el contrato.

En segundo lugar, con la adopción de medidas una vez que el contrato ha sido suscrito por el cliente, se pretenden mitigar los efectos de eventuales abusos de poder del proveedor que ha impuesto sus propias condiciones de adhesión. Tendrán lugar ante los órganos juzgadores competentes y son, esencialmente:

---

consumidores, sino durante un procedimiento de licitación de software como servicio (SaaS) de procesadores de texto para todos los departamentos del gobierno federal estadounidense. *Google* afirmó poseer la acreditación de la *Federal Information Security Management Act* para su servicio *Google Apps for Government*, cuando en realidad esta certificación cubría un servicio diferente (*Google Apps Premier*). Todo ello dentro de una disputa con *Microsoft* por la concesión de estos servicios gubernamentales, en la cual *Google* argumentaba que las condiciones de la licitación no habían sido suficientemente abiertas. Se trata del caso *Google Inc v. The United Statesand Softchoice Corporation,* núm. 10743-C.

64 En relación con contratos *cloud*, puede ser el caso de la ocultación de la existencia de otros proveedores de quienes dependa la disponibilidad del servicio, los riesgos que puede implicar para el consumidor el uso del servicio (por ejemplo, para sus datos personales o críticos), o la exclusión de responsabilidades que puedan dejar al proveedor de la nube exento de responder por cualquier incidencia relacionada con el servicio.

65 Son muchos los software como servicio y las plataformas web 2.0 que permiten la suscripción de servicios a menores de 18 años sin autorización paterna, como las redes sociales, los servicios de videojuegos en línea o servicios de correo electrónico, entre otros.

66 Puesto que la inmensa mayoría de consumidores contrata en línea sus servicios *cloud*, les será de aplicación la LSSI y no la LOCM, quedando esta desplazada por el carácter especial de aquella.

67 Algunas de ellas subsidiarias (Código Civil) y otras específicas de ciertos sectores (Ley 22/2007 de Contratación a Distancia de Servicios Financieros).

a) a modo de control de incorporación[68], la exigencia de acceso al contenido de las condiciones generales y su transparencia y claridad en la redacción de las cláusulas propuestas al consumidor, recogida por los artículos 5 y 7 de la Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación[69], y 80.1 del TRDCU[70]. Se pretende con esta regulación, que las condiciones generales se redacten de tal manera que se permita al adherente tener conocimiento de las implicaciones de la suscripción del contrato[71].

---

68 En palabras de LLODRÁ GRIMALT, "el control de incorporación [de las condiciones generales de contratación] al contrato es un mecanismo articulado en una serie de reglas cuya finalidad es decidir si las condiciones generales de contratación se han incorporado al contrato por haber cumplido unos determinados requisitos, que representan una concreción del deber de buena fe que las partes contratantes tienen en la fase previa o preliminar del contrato". Entre estos requisitos, se encuentran la plasmación documental (que se hallen en el texto del contrato o que hagan referencia al documento que las contiene), el deber de entregar copia al adherente; el requisito de firma; y que estén formuladas con transparencia, concreción y sencillez; LLODRÁ GRIMALT; Francisca; *El contrato celebrado bajo condiciones generales*, Valencia, 2002, págs. 259, 274 a 310. Asimismo, ver ALFARO AGUILA-REAL, Jesús, "Cláusulas abusivas, cláusulas predispuestas y condiciones generales", *Anuario Jurídico de La Rioja*, núm. 4, 1998, págs. 53 a 70, y ALFARO ÁGUILA-REAL, Jesús, *Las condiciones generales de la contratación. Estudio de las disposiciones generales,* 1ª edición, Madrid, 1991, 482 págs.

69 Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación, art. 5: "1. Las condiciones generales pasarán a formar parte del contrato cuando se acepte por el adherente su incorporación al mismo y sea firmado por todos los contratantes. Todo contrato deberá hacer referencia a las condiciones generales incorporadas. No podrá entenderse que ha habido aceptación de la incorporación de las condiciones generales al contrato cuando el predisponente no haya informado expresamente al adherente acerca de su existencia y no le haya facilitado un ejemplar de las mismas. 2. (...) 3. En los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma.4. La redacción de las cláusulas generales deberá ajustarse a los criterios de transparencia, claridad, concreción y sencillez", y art. 7: "No quedarán incorporadas al contrato las siguientes condiciones generales: a) Las que el adherente no haya tenido oportunidad real de conocer de manera completa al tiempo de la celebración del contrato o cuando no hayan sido firmadas, cuando sea necesario, en los términos resultantes del artículo 5. b) Las que sean ilegibles, ambiguas, oscuras e incomprensibles, salvo, en cuanto a estas últimas, que hubieren sido expresamente aceptadas por escrito por el adherente y se ajusten a la normativa específica que discipline en su ámbito la necesaria transparencia de las cláusulas contenidas en el contrato".

70 Art. 80.1 TRDCU: "En los contratos con consumidores y usuarios que utilicen cláusulas no negociadas individualmente, (...), aquéllas deberán cumplir los siguientes requisitos: a) Concreción, claridad y sencillez en la redacción, con posibilidad de comprensión directa, sin reenvíos a textos o documentos que no se faciliten previa o simultáneamente a la conclusión del contrato, y a los que, en todo caso, deberá hacerse referencia expresa en el documento contractual. b) Accesibilidad y legibilidad, de forma que permita al consumidor y usuario el conocimiento previo a la celebración del contrato sobre su existencia y contenido. En ningún caso se entenderá cumplido este requisito si el tamaño de la letra del contrato fuese inferior al milímetro y medio o el insuficiente contraste con el fondo hiciese dificultosa la lectura".

71 En la práctica, a menudo los consumidores no leen o no se interesan en comprender los contenidos de los contratos de adhesión. Así lo revelan ciertos estudios, como el informe sobre

b) la aplicación de la ley del lugar de residencia del consumidor[72], y la posibilidad de interponer acciones en los tribunales también en su lugar de residencia[73];

---

comportamiento del consumidor ante información estandarizada adoptada bajo la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a una normativa común de compraventa europea (*Common European Sales Law*), realizado en octubre de 2013 por *The Gallup Organization* a petición de la Unión Europea, y que lleva por título "*Testing of a Standardised Information Notice for Consumers on the Common European Sales Law*" [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/files/common_sales_law/cesl_gallup_consortium_final_report_en.pdf>. [Fecha de consulta: 20 de abril de 2017].

72 Art. 6 del Reglamento CE nº 593/2008 del Parlamento Europeo y del Consejo, de 17 de junio de 2008, sobre la ley aplicable a las obligaciones contractuales: "1. Sin perjuicio de los artículos 5 y 7, el contrato celebrado por una persona física para un uso que pueda considerarse ajeno a su actividad comercial o profesional («el consumidor») con otra persona («el profesional») que actúe en ejercicio de su actividad comercial o profesional, se regirá por la ley del país en que el consumidor tenga su residencia habitual, siempre que el profesional: a) ejerza sus actividades comerciales o profesionales en el país donde el consumidor tenga su residencia habitual, o b) por cualquier medio dirija estas actividades a ese país o a distintos países, incluido ese país, y el contrato estuviera comprendido en el ámbito de dichas actividades. 2. No obstante lo dispuesto en el apartado 1, las partes podrán elegir la ley aplicable a un contrato que cumple los requisitos del apartado 1, de conformidad con el artículo 3. Sin embargo, dicha elección no podrá acarrear, para el consumidor, la pérdida de la protección que le proporcionen aquellas disposiciones que no puedan excluirse mediante acuerdo en virtud de la ley que, a falta de elección, habría sido aplicable de conformidad con el apartado 1.(...)".

73 Arts. 15 a 17 del Reglamento CE 44/2001 del Consejo, de 22 de diciembre del 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (Bruselas I): "Art. 15: 1. En materia de contratos celebrados por una persona, el consumidor, para un uso que pudiere considerarse ajeno a su actividad profesional, la competencia quedará determinada por la presente sección, (…) c) en todos los demás casos, cuando la otra parte contratante ejerciere actividades comerciales o profesionales en el Estado miembro del domicilio del consumidor o, por cualquier medio, dirigiere tales actividades a dicho Estado miembro o a varios Estados miembros, incluido este último, y el contrato estuviere comprendido en el marco de dichas actividades. 2. Cuando el cocontratante del consumidor no estuviere domiciliado en un Estado miembro, pero poseyere una sucursal, agencia o cualquier otro establecimiento en un Estado miembro, se considerará para todos los litigios relativos a su explotación que está domiciliado en dicho Estado.(...) Artículo 16: 1. La acción entablada por un consumidor contra la otra parte contratante podrá interponerse ante los tribunales del Estado miembro en que estuviere domiciliada dicha parte o ante el tribunal del lugar en que estuviere domiciliado el consumidor. 2. La acción entablada contra el consumidor por la otra parte contratante sólo podrá interponerse ante los tribunales del Estado miembro en que estuviere domiciliado el consumidor. (…) Artículo 17: Únicamente prevalecerán sobre las disposiciones de la presente sección los acuerdos atributivos de competencia: 1. posteriores al nacimiento del litigio; o 2. que permitieren al consumidor formular demandas ante tribunales distintos de los indicados en la presente sección; o 3. que habiéndose celebrado entre un consumidor y su cocontratante, domiciliados o con residencia habitual en el mismo Estado miembro en el momento de la celebración del contrato, atribuyeren competencia a los tribunales de dicho Estado miembro, a no ser que la ley de éste prohibiere tales acuerdos", y 22.4 de la LOPJ: "Asimismo, en materia de contratos de consumidores, cuando el comprador tenga su domicilio en España si se trata de una venta a plazos de objetos muebles corporales o de préstamos destinados a financiar su adquisición; y en el caso de cualquier otro contrato de prestación de servicio o relativo a bienes muebles, cuando la celebración del contrato hubiere sido precedida por oferta personal o de publicidad realizada en España o el consumidor hubiera llevado a cabo en territorio español los

c) el reconocimiento del derecho de desistimiento del artículo 68 TRDCU[74];

d) el establecimiento de presunciones en favor del consumidor, como la interpretación de las cláusulas según el principio "*in dubio, pro consumatore",* reconocido en el artículo 51 de nuestra Constitución[75] y en el art. 80.2 del TRDCU[76]; y la interpretación atendiendo a la naturaleza del servicio, a las circunstancias de celebración y a la dependencia de otros pactos, establecidos por el art. 82.3 del TRDCU[77].

d) el control del contenido de las cláusulas de adhesión: la apreciación, en primer lugar, de su legalidad (art. 6.3, 1255, 1271 y 1275 del Código Civil), y, en segundo lugar, de su eventual carácter abusivo de las cláusulas según los términos de los apartados 1 y 4 del art. 82 del TRDCU[78] y los artículos 85 a 91 de la Directiva

---

actos necesarios para la celebración del contrato; en materia de seguros, cuando el asegurado y asegurador tengan su domicilio en España; y en los litigios relativos a la explotación de una sucursal, agencia o establecimiento mercantil, cuando éste se encuentre en territorio español. En materia concursal se estará a lo dispuesto en su ley reguladora".

74 Art. 68 TRDCU: "El derecho de desistimiento de un contrato es la facultad del consumidor y usuario de dejar sin efecto el contrato celebrado, notificándoselo así a la otra parte contratante en el plazo establecido para el ejercicio de ese derecho, sin necesidad de justificar su decisión y sin penalización de ninguna clase. Serán nulas de pleno de derecho las cláusulas que impongan al consumidor y usuario una penalización por el ejercicio de su derecho de desistimiento. 2. El consumidor tendrá derecho a desistir del contrato en los supuestos previstos legal o reglamentariamente y cuando así se le reconozca en la oferta, promoción publicidad o en el propio contrato. 3. El derecho de desistimiento atribuido legalmente al consumidor y usuario se regirá en primer término por las disposiciones legales que lo establezcan en cada caso y en su defecto por lo dispuesto en este Título".

75 Art. 51 de la Constitución Española: "1. Los poderes públicos garantizarán la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces, la seguridad, la salud y los legítimos intereses económicos de los mismos. 2. Los poderes públicos promoverán la información y la educación de los consumidores y usuarios, fomentarán sus organizaciones y oirán a esta en las cuestiones que puedan afectar a aquéllos, en los términos que la Ley establezca. 3. En el marco de lo dispuesto por los apartados anteriores, la Ley regulará el comercio interior y el régimen de autorización de productos comerciales".

76 Art. 80.2 TRDCU: "Cuando se ejerciten acciones individuales, en caso de duda sobre el sentido de una cláusula prevalecerá la interpretación más favorable al consumidor".

77 Art. 82.3 TRDCU: "El carácter abusivo de una cláusula se apreciará teniendo en cuenta la naturaleza de los bienes o servicios objeto del contrato y considerando todas las circunstancias concurrentes en el momento de su celebración, así como todas las demás cláusulas del contrato o de otro del que éste dependa".

78 Art. 82.1 TRDCU: "Se considerarán cláusulas abusivas todas aquellas estipulaciones no negociadas individualmente y todas aquéllas prácticas no consentidas expresamente que, en contra de las exigencias de la buena fe causen, en perjuicio del consumidor y usuario, un desequilibrio importante de los derechos y obligaciones de las partes que se deriven del contrato." Art. 82.4 TRDCU: "No obstante lo previsto en los apartados precedentes, en todo caso son abusivas las cláusulas que, conforme a lo dispuesto en los artículos 85 a 90, ambos inclusive: a) vinculen el contrato a la voluntad del empresario, b) limiten los derechos del consumidor y usuario, c) determinen la falta de reciprocidad en el contrato, d) impongan al consumidor y usuario garantías desproporcionadas o le impongan indebidamente la carga de la prueba, e) resulten desproporcionadas en relación con el perfeccionamiento y ejecución del contrato, o f) contravengan las reglas sobre competencia y derecho aplicable".

93/13/CE[79]. De de acuerdo con los concretos contenidos calificados como abusivos en los artículos 8 a 10 de la Ley de Condiciones Generales de la Contratación y 82 a 91 del TRLGDCU, las cláusulas que se declaren abusivas tendrán como efecto la nulidad, aunque hayan sido conocidas y aceptadas por el consumidor, y se entenderán como no puestas en el contrato, aunque el resto del contrato puede subsistir (arts. 8.2, 9.1 y 10.1 de la Ley de Condiciones Generales de la Contratación, y art. 83 de la TRDCU, en la redacción dada por la Ley 3/2014 de 27 de marzo[80])[81];

e) la consecuente determinación de responsabilidad por incumplimientos contractuales, falta de diligencia del proveedor, etc., que hayan podido causar daños o perjuicios al consumidor o a terceros, en los artículos 118 a 146 del TRDCU.

Por otro lado, los códigos de buenas prácticas adoptados voluntariamente por los proveedores pueden ser un buen mecanismo para suavizar posibles situaciones de indefensión de suscriptores de servicios (sean o no consumidores) y eventuales abusos del proveedor *cloud*[82]. Igualmente, existen iniciativas europeas especialmente dirigidas a la protección al destinatario de servicios de computación en la nube y de

79 Arts. 2 y 3 Directiva 91/13/CEE: "A efectos de la presente Directiva se entenderá por: a) « cláusulas abusivas »: las cláusulas de un contrato tal como quedan definidas en el artículo 3;b) « consumidor »: toda persona física que, en los contratos regulados por la presente Directiva, actúe con un propósito ajeno a su actividad profesional; c) « profesional »: toda persona física o jurídica que, en las transacciones reguladas por la presente Directiva, actúe dentro del marco de su actividad profesional, ya sea pública o privada. Artículo 31. Las cláusulas contractuales que no se hayan negociado individualmente se considerarán abusivas si, pese a las exigencias de la buena fe, causan en detrimento del consumidor un desequilibrio importante entre los derechos y obligaciones de las partes que se derivan del contrato. 2. Se considerará que una cláusula no se ha negociado individualmente cuando haya sido redactada previamente y el consumidor no haya podido influir sobre su contenido, en particular en el caso de los contratos de adhesión. El hecho de que ciertos elementos de una cláusula o que una cláusula aislada se hayan negociado individualmente no excluirá la aplicación del presente artículo al resto del contrato si la apreciación global lleva a la conclusión de que se trata, no obstante, de un contrato de adhesión. El profesional que afirme que una cláusula tipo se ha negociado individualmente asumirá plenamente la carga de la prueba. 3. El Anexo de la presente Directiva contiene una lista indicativa y no exhaustiva de cláusulas que pueden ser declaradas abusivas".

80 Art. 83 TRDCU: "Las cláusulas abusivas serán nulas de pleno derecho y se tendrán por no puestas. A estos efectos, el Juez, previa audiencia de las partes, declarará la nulidad de las cláusulas abusivas incluidas en el contrato, el cual, no obstante, seguirá siendo obligatorio para las partes en los mismos términos, siempre que pueda subsistir sin dichas cláusulas".

81 Dedicaremos un estudio más detallado de esta cuestión en el apartado "Responsabilidad directa del proveedor: limitaciones y exoneraciones. La aceptación de los servicios "tal cual están" y "según estén disponibles" ("*as is*" y "*as available*")", recogido en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

82 El organismo *Cloud Industry Forum* ha creado la iniciativa *Code of Practice for Cloud Computing Providers*, junto con la concesión de una certificación anual que acredita su cumplimiento. Disponible en: <http://cloudindustryforum.org/code-of-practice/code-of-practice> [Fecha de consulta: 15 de enero de 2015].

aplicaciones informáticas, como la Propuesta de Directiva de compraventa en línea y otras ventas a distancia[83], y la Propuesta de Directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales[84].

Hemos expuesto en este apartado la normativa aplicable a los consumidores, lo cual no implica que no pueda aplicarse de manera analógica a profesionales que puedan asimilar su situación a la del consumidor. En posteriores capítulos se planteará cómo, en ocasiones, tanto el profesional independiente como el pequeño y mediano empresario que integran el suministro dentro de la operativa diaria de su negocio, pueden verse injustamente desprotegidos en la contratación de servicios de computación remota. La posición de inferioridad de estos actores respecto de la empresa proveedora de servicios *cloud* se puede poner en equivalencia con la del consumidor, por cuanto, como hemos mencionado, no tienen posibilidad de negociar las cláusulas impuestas por el proveedor (independientemente de que el servicio sea gratuito o de pago)[85].

Debemos añadir que, al igual que sucede con la mayoría de consumidores, muchos de estos profesionales y empresas que se posicionan como usuarios finales de servicios *cloud,* no leen detenidamente las cláusulas de los contratos en línea, ya sea porque necesitan ese concreto servicio y no pueden sustituirlo por ninguno similar y/o porque lo requieren de forma inmediata, ya sea porque consideran que su falta de experiencia y conocimientos en materia informática y legal serán insuficientes para comprender unas condiciones muchas veces poco claras o excesivamente técnicas[86].

---

83 El artículo 1 de la Propuesta establece la finalidad de esta Directiva: "La presente Directiva establece algunos requisitos sobre determinados aspectos de los contratos de compraventa a distancia celebrados entre el vendedor y el consumidor, en particular las normas sobre la conformidad del producto, los saneamientos en caso de no conformidad y las modalidades para el ejercicio de dichos saneamientos".

84 El contenido general de la regulación de esta Directiva se establece en el artículo 1 de su Propuesta. "La presente Directiva establece algunos requisitos sobre determinados aspectos de los contratos de compraventa a distancia celebrados entre el vendedor y el consumidor, en particular las normas sobre la conformidad del producto, los saneamientos en caso de no conformidad y las modalidades para el ejercicio de dichos saneamientos". Nos remitimos, para un análisis detallado, a MILÁ RAFEL, Rosa; "Intercambios digitales en Europa: Las propuestas de Directiva sobre compraventa en línea y suministro de contenidos digitales", *Revista CESCO de Derecho de Consumo*, núm. 17, 2016, págs 11-44; y FERNÁNDEZ MASIÁ, Enrique; "Optando por la normativa común de compraventa europea"; *Revista Electrónica de Estudios Internacionales*, núm. 23, 2012.

85 Ver apartado "Breve reflexión relativa a la aplicación extensiva de las normas y criterios sobre cláusulas abusivas al pequeño empresario", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

86 Así lo revela el estudio sobre comportamiento del consumidor ante información estandarizada, realizado en octubre de 2013 por *The Gallup Organization* a petición de la Unión Europea, y que

Consideramos que sería deseable que los juzgadores extendiesen analógicamente, si bien no toda, al menos parte de la protección que se destina al consumidor, a aquellos profesionales y pequeños empresarios sin capacidad para negociar el contrato, cuando sea constatable que su situación de indefensión es similar a la del consumidor. A nuestro parecer, puede determinarse que existe tal indefensión en aquellos casos en los que el adherente profesional se encuentra en evidente situación de desventaja económica con el proveedor y que carece de conocimientos tecnológicos y/o jurídicos[87]. Así, no se dejaría a la voluntad del proveedor el contenido de la relación contractual. El proveedor, en ocasiones, excluye parte de su responsabilidad por el funcionamiento del servicio *cloud*[88] e introduce cláusulas manifiestamente abusivas a sabiendas de que el usuario profesional, a diferencia del usuario consumidor[89], no podrá exigir que se declare su

---

lleva por título "*Testing of a Standardised Information Notice for Consumers on the Common European Sales Law*" [en línea], <http://ec.europa.eu/justice/contract/files/common_sales_law/cesl_gallup_consortium_final_report_en.pdf>. [Fecha de consulta: 24 de abril de 2017]. Cada vez más, los proveedores de software como servicio se esfuerzan por extender sus condiciones generales en términos casi coloquiales, redactados en segunda persona, con ejemplos prácticos de las responsabilidades y exclusiones de responsabilidad, huyendo de tecnicismos, para hacerlos comprensibles al máximo número de sus usuarios. Por ejemplo, las condiciones de diferentes servicios de Google.

87 En la Exposición de Motivos de la Ley 17/1998 sobre Condiciones Generales de la Contratación se reconoce que con las cláusulas de adhesión también pueden lesionarse los intereses de personas jurídicas y de profesionales: "La protección de la igualdad de los contratantes es presupuesto necesario de la justicia de los contenidos contractuales y constituye uno de los imperativos de la política jurídica en el ámbito de la actividad económica. Por ello la Ley pretende proteger los legítimos intereses de los consumidores y usuarios, pero también de cualquiera que contrate con una persona que utilice condiciones generales en su actividad contractual. (…) Esto no quiere decir que en las condiciones generales entre profesionales no pueda existir abuso de una posición dominante. Pero tal concepto se sujetará a las normas generales de nulidad contractual. Es decir, nada impide que también judicialmente pueda declararse la nulidad de una condición general que sea abusiva cuando sea contraria a la buena fe y cause un desequilibrio importante entre los derechos y obligaciones de las partes, incluso aunque se trate de contratos entre profesionales o empresarios. Pero habrá de tener en cuenta en cada caso las características específicas de la contratación entre empresas".

88 Ver capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

89 Seguidamente enunciaremos las cláusulas que, en nuestra opinión, son más relevantes para el usuario final de servicios de computación en la nube: a) la legislación aplicable y la jurisdicción competente; b) las políticas de uso adecuado del servicio (en adelante, PUA); c) las variaciones de las condiciones contractuales; d) la tarifación de los servicios y los mecanismos de pago; e) las cláusulas relativas a integridad y confidencialidad de los datos y a su ubicación y transferencia, especialmente en cuanto a datos personales; f) la monitorización de sus actividades como usuario del servicio y del consumo de servicios a efectos de determinación des acuerdo de nivel de servicio y de la tarifa devengada; g) las cesiones de derechos de propiedad intelectual sobre los datos al proveedor; h) la cesión de cierta información del cliente a terceros, por parte del proveedor, por

no incorporación o nulidad por vía judicial más que por los cauces de los artículos 7[90] y 8.1[91] de la Ley de Condiciones Generales de la Contratación y por el artículo 6.3 del Código Civil[92].

Respecto de esta cuestión, y en concreto, en cuanto a la calificación de una condición general incluida en un contrato de adhesión de servicios de computación en la nube como cláusula abusiva y su ineficacia ante adherentes consumidores y, eventualmente, ante adherentes que sean pequeños empresarios o profesionales, nos remitimos a capítulos posteriores[93].

3.3.- Las Administraciones Públicas

Anteriormente hemos comentado la estrategia *European Cloud Computing Strategy* adoptada por la Comisión Europea, que juega un papel primordial en el impulso y adopción de la computación en la nube por el sector público[94]. El

---

ejemplo con fines publicitarios; i) la garantías de fiabilidad de la prestación; j) las posibles exclusiones y limitaciones de responsabilidad del proveedor por pérdida de datos almacenados en la nube, porque puedan verse comprometidos, por la imposibilidad de acceder a ellos, por daños causados en equipos, etc.; k) las indemnizaciones al proveedor y a terceros por daños ocasionados por el consumidor; y l) otras cuestiones de interés: avisos y recomendaciones de seguridad, necesidad de contratar servicios accesorios, etc. La mayoría de estas cláusulas tendrán su propio tratamiento en posteriores capítulos de este trabajo, desde la perspectiva de su suscripción por el pequeño empresario.

90 El art. 7 de la Ley 17/1998 establece como no puestas las cláusulas de adhesión no accesibles o poco transparentes, también para adherentes no consumidores: "No quedarán incorporadas al contrato las siguientes condiciones generales: a) Las que el adherente no haya tenido oportunidad real de conocer de manera completa al tiempo de la celebración del contrato o cuando no hayan sido firmadas, cuando sea necesario, en los términos resultantes del artículo 5. b) Las que sean ilegibles, ambiguas, oscuras e incomprensibles, salvo, en cuanto a estas últimas, que hubieren sido expresamente aceptadas por escrito por el adherente y se ajusten a la normativa específica que discipline en su ámbito la necesaria transparencia de las cláusulas contenidas en el contrato".

91 El art. 8.1 de la ley 17/1998 de Condiciones Generales de la Contratación establece la nulidad para cuando el contratante no tenga la consideración de consumidor: "Serán nulas de pleno derecho las condiciones generales que contradigan en perjuicio del adherente lo dispuesto en esta Ley o en cualquier otra norma imperativa o prohibitiva, salvo que en ellas se establezca un efecto distinto para el caso de contravención".

92 El imperativo del art. 6.3 del Código Civil dice: "Los actos contrarios a las normas imperativas y a las prohibitivas son nulos de pleno derecho, salvo que en ellas se establezca un efecto distinto para el caso de contravención".

93 Ver apartado "Responsabilidad directa del proveedor: limitaciones y exoneraciones. La aceptación de los servicios "tal cual están" y "según estén disponibles" ("*as is*" y "*as available*")", recogido en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

94 En la web de la Comisión Europea aparece información sobre el contenido y desarrollo de esta estrategia. Disponible en: <http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy>. [Fecha de consulta: 24 de abril de 2017].

Ministerio de Hacienda y Administraciones Públicas forma parte del Comité Ejecutivo del *European Cloud Parternship* creado por la Comisión Europea para la implantación de la *Cloud Computing Stategy*[95]. Con esta estrategia se pretende alcanzar una implementación de redes que sean compatibles e interoperativas, facilitando el intercambio de información y el acceso a los servicios públicos de instituciones nacionales de los Estados miembros e instituciones europeas.

En relación con la Administración como contratante de servicios de computación en nube, la *Cloud Computing Stategy* europea promociona el desarrollo de requisitos comunes de adjudicación de suministros *cloud*, sujetándolos a ciertas condiciones técnicas y a los principios de no discriminación de empresas provenientes de otros Estados miembros y de transparencia aplicables a cualquier contrato del sector público[96]. Además, deben abstenerse de hacer referencia a marcas comerciales o patentes concretas al describir las características de los productos y servicios que desean adquirir[97]; y están obligados a aceptar los documentos

95 Esta estrategia nació en el año 2012, a partir de la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Liberar el potencial de la computación en nube en Europa. COM (2012) 539 final. Se diseñó para impulsar el uso de la tecnología de la computación en la nube en todos los sectores económicos, y aprovechar al máximo su potencial. Para ello se establecieron tres ámbitos de actuación: el desarrollo de cláusulas contractuales modelo a modo de buenas prácticas; desarrollar estándares técnicos de interoperabilidad, portabilidad y reversibilidad; y establecer un sistema de cooperación entre industria del sector *cloud* y el sector público para aumentar la confianza en el uso de estos servicios. Disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:ES:PDF> y <https://ec.europa.eu/digital-single-market/en/european-cloud-computing-strategy>. [Fecha de consulta: 24 de abril de 2017].

96 El régimen de adjudicación pública de la Unión Europea está comprendido por las Directivas 2014/24/UE sobre contratación pública, 2014/25/CE sobre la contratación por entidades que operan en los sectores del agua, de la energía, de los transportes y de los servicios postales; y 2009/81/CE sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios por las entidades o poderes adjudicadores en los ámbitos de la defensa y la seguridad.

97 Es importante, para garantizar la entrada de empresas tecnológicas, que no se exijan especificaciones basadas en juicios de valor y que pueden beneficiar a un proveedor determinado, sino que debe apostarse por exigencias y estándares de carácter abierto. En octubre de 2010 Google demandó al Departamento de Interior americano alegando distorsión ilegal de la competencia, al exigir, en relación a la licitación de un contrato de servicios TIC por valor de 59 millones de $, que la mensajería debía basarse en la *Microsoft Bussiness Productivity Online Suite,* con lo cual se privaba a la demandante de la oportunidad de competir, al exigirse requisitos que solo podía proporcionar otra marca comercial, beneficiada por tanto por tal predilección fruto, a tenor de la sentencia, de los *network effects*. En febrero de 2011 la juez Susan Braden de la *US Court of Federal Claims of Washington* declaró que efectivamente se habían violado las normas sobre

justificativos (certificados, titulaciones, etc.) expedidos por otro país de la UE, siempre que ofrezcan el mismo nivel de garantía deben poner toda la información relativa a las licitaciones a disposición de cualquier empresa interesada, con independencia de cuál sea el país de la UE en el que esté registrada[98].

La Comisión Europea también colabora con otros organismos, como el *Cloud Industry Forum*[99], un consorcio de Administraciones Públicas de once países miembros (entre los que se encuentra España), entidades de estandarización y representantes de la industria privada que pretenden identificar las necesidades del sector público y desarrollar e implementar soluciones innovadoras basadas en la tecnología de la nube, como el almacenamiento seguro en la nube de legislación. Para esta licitación conjunta se pretenden establecer, además, unas adecuadas condiciones contractuales para las futuras concesiones públicas de servicios *cloud.*

En el contexto normativo español, la entrada en vigor de la Ley 11/2007 de 22 de junio, de acceso a los ciudadanos a los Servicios Públicos, supuso un punto de no retorno en la introducción de novedades tecnológicas en el ámbito administrativo. Su artículo 33[100] permite utilizar la computación en la nube tanto en las relaciones con los administrados como en la tramitación y documentación de procedimientos[101].

En cuanto a los procedimientos de adjudicación de los contratos públicos de servicios *cloud* y su adecuación al régimen legal español actual, las administraciones deben posibilitar el mayor número de potenciales suministradores, para asegurar un

---

competencia y obligó a la demandada a modificar los criterios de licitación. Este documento está disponible en línea: <http://www.uscfc.uscourts.gov/sites/default/files/opinions/Google%20PI%20Redacted.pdf>. [Fecha de consulta: 24 de abril de 2017].

98 Estas condiciones para la licitación se han extractado de su publicación la página web oficial de la Unión Europea: <http://europa.eu/youreurope/business/public-tenders/rules-procedures/index_es.htm>. [Fecha de consulta: 24 de abril de 2017].

99 Sitio web del Cloud Industry Forum , disponible en: <http://www.cloudforeurope.eu/home>. [Fecha de consulta: 24 de abril de 2017].

100 Artículo 33 de la Ley 11/2007 de 22 de junio, de acceso a los ciudadanos a los Servicios Públicos: "La gestión electrónica de la actividad administrativa respetará la titularidad y el ejercicio de la competencia por la Administración Pública, órgano o entidad que la tenga atribuida y el cumplimiento de los requisitos formales y materiales establecidos en las normas que regulen la correspondiente actividad. A estos efectos, y en todo caso bajo criterios de simplificación administrativa, se impulsará la aplicación de medios electrónicos a los procesos de trabajo y la gestión de los procedimientos y de la actuación administrativa".

101 PALOMAR OLMEDA, Alberto; "Incidencia del *Cloud Computing* en el ámbito de la contratación pública", *Derecho y Cloud Computing* (Ed. Ricard Martínez), 1ª edición, Navarra, 2012, págs. 201 a 230.

mercado competitivo[102]. Respecto del nacimiento de responsabilidades de las Administraciones Públicas, el artículo 214 del Texto Refundido de la Ley de Contratos del Sector Público[103] establece la obligación del contratista de indemnizar todos los daños y perjuicios que se causen a terceros como consecuencia de la ejecución del contrato (como podrían ser, en nuestro caso, el mal funcionamiento del hardware o de los servicios *cloud* de infraestructura (IaaS) o los problemas derivados del diseño o incompatibilidades de las aplicaciones de software como servicio (SaaS) y del uso distinto al estrictamente necesario para la ejecución del contrato de la información administrativa a la cual ha tenido acceso[104]. El contratista no responderá de aquellos daños provocados por el contratista a consecuencia del cumplimiento de las instrucciones exigidas por la Administración, de acuerdo con el mismo artículo 214 del Texto Refundido de la Ley de Contratos del Sector Público. La Administración, por su parte, debe asegurarse de conocer los riesgos de la externalización de sus servicios a través de contratos de computación en la nube y de que los proveedores escogidos aportan las suficientes garantías en cuanto a la seguridad de la información y cumplen con las exigencias de la normativa aplicable[105].

Por último, cabe mencionar que el contrato de computación en la nube, en el

---

102 La normativa aplicable vigente actualmente es fundamentalmente, la que sigue: Texto refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre; Ley 31/2007, de 30 de octubre, sobre procedimientos de contratación en los sectores del agua, la energía, los transportes y los servicios postales; Real Decreto 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas y el Real Decreto 817/2009, de 8 de mayo, por el que se desarrolla parcialmente la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público. En Baleares, además, rigen la Ley 3/2003, de 26 de marzo, de Régimen jurídico de la Administración de la Comunidad Autónoma de las Illes Balears y el Decreto 147/2000, de 10 de noviembre, sobre contratación de la Comunidad Autónoma de las Illes Balears. En breve se verán modificadas estas normas porque deben transponerse las nuevas Directivas 2014/24/CE y 2014/25CE aprobadas recientemente.

103 Art. 214 del Texto Refundido de la Ley de Contratos del Sector Público: "Será obligación del contratista indemnizar todos los daños y perjuicios que se causen a terceros como consecuencia de las operaciones que requiera la ejecución del contrato. 2. Cuando tales daños y perjuicios hayan sido ocasionados como consecuencia inmediata y directa de una orden de la Administración, será ésta responsable dentro de los límites señalados en las Leyes. También será la Administración responsable de los daños que se causen a terceros como consecuencia de los vicios del proyecto elaborado por ella misma en el contrato de obras o en el de suministro de fabricación".

104 VALERO TORRIJOS, Julián, "La Administración Pública en la nube. Análisis de las implicaciones jurídicas desde la normativa sobre Administración electrónica", *Derecho y Cloud Computing* (Ed. Ricard Martínez), 1ª edición, Navarra, 2012, pág. 249.

105 VALERO TORRIJOS, Julián, *op. cit.* pág. 252.

régimen legal administrativo, y más concretamente, en el artículo 9 del Texto Refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre, se considera un contrato de suministro[106]. Como hemos manifestado en el capítulo anterior, la naturaleza jurídica del suministro no se adecua, en nuestra opinión, al contrato de computación en la nube suscrito por empresas privadas y particulares, siendo más adecuado categorizarlo como contrato de servicios, discusión que se extiende también al propio ámbito administrativo[107].

Como apuntan acertadamente ciertos autores, el contrato suscrito entre proveedor *cloud* y Administración Pública podría ser igualmente un contrato de adhesión de nube pública, e incluso de servicios sin contraprestación monetaria; independientemente de la idoneidad de estos servicios en cuanto a la seguridad de datos especialmente sensibles, la Administración debería responder por daños derivados de esta relación contractual, y repetir contra el proveedor en aquellos casos en los que el daño se hubiese provocado por una prestación defectuosa del servicio o por un incumplimiento de lo acordado[108].

4.- TERCEROS RELACIONADOS CON EL CONTRATO DE COMPUTACIÓN EN LA NUBE

Existen terceros profesionales que, aun sin haber formado parte del contrato de servicios de computación en la nube, pueden verse obligados a responder por incidencias derivadas de su ejecución. A continuación, realizamos una breve mención para el integrador de servicios tecnológicos y las entidades aseguradoras de riesgos informáticos.

4.1.- La figura del integrador de sistemas

Está aumentando en el sector informático la presencia del integrador, un

106 Art. 9 del Texto Refundido de la Ley de Contratos del Sector Público: "1. Son contratos de suministro los que tienen por objeto la adquisición, el arrendamiento financiero, o el arrendamiento, con o sin opción de compra, de productos o bienes muebles. (...) 3.- En todo caso, se considerarán contratos de suministro los siguientes: (...) b) Los que tengan por objeto la adquisición y el arrendamiento de equipos y sistemas de telecomunicaciones o para el tratamiento de la información, sus dispositivos y programas, y la cesión del derecho de uso de estos últimos, a excepción de los contratos de adquisición de programas de ordenador desarrollados a medida, que se considerarán contratos de servicios".

107 PALOMAR OLMEDA, Alberto, "Incidencia del *Cloud Computing* en el ámbito de la contratación pública", *Derecho y Cloud Computing* (Ed. Ricard Martínez), 1ª edición, Navarra, 2012, págs. 214, 218.

108 VALERO TORRIJOS, Julián, *op. cit.,* pág. 250.

intermediario que provee de servicios de consultoría sobre entornos *cloud* y asistencia personalizada a los usuarios para que migren con seguridad y eficiencia sus datos y/o aplicaciones hacia la nube[109]. Se trata de un profesional o empresa dedicada a asesorar y, en algunos casos, equipar con sistemas informáticos y de telecomunicaciones una organización o entorno y a asegurar su funcionamiento conjunto. Sus principales funciones consisten en diseñar, planificar, integrar y desplegar entornos informáticos, ya sean entornos hardware físicos o virtualizaciones y sistemas en la nube, para proporcionar al cliente el máximo aprovechamiento de recursos de computación. Además, estos profesionales poseen información sobre diferentes proveedores y pueden calibrar mejor cuál es la solución más adecuada para el cliente, con lo cual ofrecerá una visión más objetiva que la del proveedor. De esta manera, el conocimiento de diferentes productos permitirá combinar tecnologías de diferentes proveedores para conseguir el óptimo suministro para el cliente con el menor coste de componentes[110].

Por contra, existen también integradores que únicamente trabajan con un proveedor *cloud*, funcionando a modo de "partner" o comercial, con lo cual presentan un solvente nivel de conocimientos sobre esa marca concreta y sobre sus soluciones y productos[111].

Los integradores, por su parte, también pueden ser usuarios de servicios *cloud* de infraestructura (IaaS) y plataforma (PaaS), que utilizan para proporcionar servicios personalizados de software (SaaS) o para sustentar los entornos de nube privados o híbridos a medida de sus clientes finales. Asimismo, el diseño, planificación y migración hacia una solución basada en tecnología *cloud* puede formar parte de un completo paquete de servicios informáticos: ancho de banda,

---

109 En 2012, la empresa analista de mercados IDC elaboró, a petición de *Infosys* (integrador de servicios *cloud* y *outsourcing)*, un informe en el cual se revela que para el 56% de las empresas, la migración a la nube supone un reto importante y para ello consideran conveniente contratar un proveedor externo que les ayude con la estrategia de implementación de la nube. Además, la encuesta revela que para el 52% de los entrevistados es muy importante elegir los mejores proveedores *cloud* y asegurarse de la integración entre ellos. Fuente: Informe *"Adoption of Cloud: Private Cloud is Current Flavor but Hybrid Cloud is Fast Becoming a Reality"* [en línea]. Disponible en: <http://www.infosys.com/newsroom/press-releases/Pages/cloud-ecosystem-integrator.aspx>. [Fecha de consulta: 10 de marzo de 2015].

110 Son integradores de sistemas empresas como Accenture, Tecnobit, Infosys o Altran Technology. A su vez, existen muchos profesionales independientes que ejercen como integradores de sistemas informáticos.

111 Por ejemplo, el integrador español Prodware, socio comercial de Microsoft.

servicios web, asesoría técnica o legal, mantenimiento de equipos hardware, etc.

Del mismo modo que sucede con los contratos de *Outsourcing* o de implementación de nubes privadas, la adopción de una solución informática adecuada a las necesidades concretas del cliente, así como el asesoramiento personalizado durante el proceso de migración hacia la nube, exigen de un conocimiento previo, por parte del integrador, de la operativa empresarial de la entidad adherente. Consecuentemente, los contratos de integración de sistemas no suelen consistir en un conjunto de condiciones generales predispuestas en el sitio web del integrador para su adhesión, sino que en su mayoría se negociarán previamente entre las partes. Además de este contrato de asesoría, el cliente puede, bajo recomendación del integrador, suscribir en su propio nombre el contrato de computación en la nube con un proveedor *cloud*. Así, y dependiendo de si el integrador se constituye o no como un proveedor *cloud* por sí mismo, el cliente habrá suscrito un único contrato global o dos contratos independientes (asesoría del integrador y contrato del servicio con el proveedor *cloud*) para incorporar en su sistema empresarial un entorno de computación en la nube que integre más o menos servicios.

4.2.- Las entidades aseguradoras y los entornos *cloud*

Como apunte final al apartado relativo a los sujetos implicados en la contratación de servicios de computación en la nube, cabe mencionar la existencia de contratos de seguro especializados[112]. Estos, junto con mecanismos tecnológicos de seguridad y las previsiones contractuales, permiten salvaguardar al asegurado, y cubrir gran parte de las contingencias relacionadas con sus riesgos, asociándolos a coberturas que dotan de contenido económico a los activos informáticos[113].

112 El servicio de computación en la nube presenta una serie de riesgos para el cliente que decide integrarlo en su actividad comercial. Son riesgos que resultan de combinar los riesgos del uso general de Internet (cortes de suministro, decisiones de gobiernos sobre la Red, ataques de delincuentes informáticos, etc.), el riesgo de un proveedor de servicios (disponibilidad y continuidad del servicio, negligencia profesional, etc.), o el riesgo de un diseñador de programas informáticos (errores en el diseño, incompatibilidades, etc.), y supera las coberturas generales de las pólizas que cubren la llamada "responsabilidad cibernética". El resultado de esta amalgama es un seguro especializado que da cobertura a todos estos riesgos. ALARCÓN FIDALGO, Joaquín; "Cloud Computing, responsabilidad y seguro", *Revista Española de Seguros: Publicación Doctrinal de Derecho y Economía de los Seguros Privados*, núm. 153-154, 2013, págs 29 a 42.

113 Ver apartado "Riesgos que inhiben la adopción del *Cloud Computing* por parte de las

Las coberturas pueden cubrir riesgos concretos o el entorno en su conjunto[114]. Los apagones del sistema y las pérdidas de datos tienen unos costes muy elevados para todos los actores implicados, y el mayor obstáculo para el usuario es el desconocimiento de su funcionamiento interno. Además, la transparencia sobre cuestiones como eventuales contratos de suministros de infraestructuras subyacentes con otros proveedores, los detalles sobre el tratamiento de los datos del cliente o la ubicación de los centros de datos del proveedor suele brillar por su ausencia en los términos de la información precontractual que se ofrece al cliente *cloud,* como veremos en posteriores capítulos. Igualmente, puede asegurarse la responsabilidad civil de los proveedores o del cliente de la nube frente reclamaciones de consumidores o terceros por eventuales incumplimientos del deber de diligencia[115]. Asimismo, el proveedor puede contratar un seguro de responsabilidad civil para cubrir siniestros asociados a contenidos introducidos por los usuarios[116].

Por su parte, las aseguradoras pueden ser claves en la promoción de buenas prácticas entre los operadores que integran los entornos de computación en la nube, fijando condiciones previas al suscribir la póliza o para efectuar rebajas en sus cuotas. Como muestra, las certificaciones de cumplimiento de estándares de seguridad[117] o las relativas al cumplimiento de la normativa sobre protección de datos[118].

---

empresas", en el capítulo "Concepto y características técnicas de la computación en la nube".

114 La aseguradora AIG Europe Limited, (antes Chartis Europe Limited) con sucursal en España, ofrece la póliza *CiberEdge Chartis*, que cubre el potencial impacto financiero de fugas, pérdidas o violaciones de datos, crisis de TI, etc. Como se afirma en su folleto en línea, cubre inspecciones y sanciones en materia de protección de datos que sean asegurables por Ley, y los perjuicios relacionados por interrupciones de redes o fallos de seguridad o por ciberataques, o la mitigación de la pérdida de reputación de la sociedad asegurada, entre otras contingencias. Disponible en: <https://www.aig.com.es/business/business-productos-y-servicios/lineas-financieras/cyber-edge>. [Fecha de consulta: 24 de abril de 2017].

115 KUAN HON, W; MILLARD, C, "Control, Security, and Risk in the Cloud", *Cloud Computing Law,* (Coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 34.

116 RIBAS ALEJANDRO, Javier; Aspectos jurídicos del comercio electrónico en Internet, 1ª edición, Pamplona, 1999, 294 págs, pág 158.

117 Como la certificación *ISO 27001/27002*, un estándar internacional para la seguridad de la información con carácter general. Por su parte, la matriz de controles en la nube (*CCM*, del inglés *Cloud Controls Matrix*) de la *Cloud Security Alliance* se ha diseñado para proporcionar principios de seguridad fundamentales que guíen a los proveedores de servicios en la nube y ayuden a los clientes a evaluar el riesgo de seguridad general de dichos proveedores.

118 El *PCI DSS* (*Payment Card Industry-Data Security Standards*) es un estándar para la seguridad de la información diseñado para impedir el fraude a través de controles estrictos de los datos de las tarjetas de crédito.

Capítulo Cuarto

ASPECTOS JURÍDICOS DE LOS CONTENIDOS ALOJADOS EN LA NUBE

1.- INTRODUCCIÓN

Debido a que la naturaleza de los servicios de computación en la nube a menudo exige la migración de datos hacia múltiples ubicaciones físicas y virtuales, se produce irremediablemente para el cliente, sea empresa o particular, la pérdida de control sobre uno de sus activos fundamentales[1]. Por esta razón, existen actividades poco idóneas para su implementación en infraestructuras de nube pública, como aquellas que requieran un control absoluto del entorno o que impliquen el manejo de datos críticos o altamente sensibles. En estos casos, el cliente deberá valorar la opción de implementar nubes privadas o híbridas, que minimicen los riesgos de seguridad y permitan un mayor grado de gobierno del entorno[2].

1 Como hemos mencionado en el capítulo "Concepto y características técnicas de la computación en la nube", los datos migrados a la nube se van replicando en múltiples máquinas virtuales y/o servidores que pueden estar geográficamente dispersos. Esta constante redundancia permite al proveedor no solo optimizar los costes operativos, sino también asegurar la máxima disponibilidad del servicio cuando se realizan tareas de mantenimiento u ocurren fallos de hardware o catástrofes que puedan inutilizar un determinado centro de datos.

2 En cuanto a los aspectos relacionados con la seguridad de los contenidos, este tema será tratado de manera detallada como parte de las obligaciones del proveedor, en el capítulo "Obligaciones y

CAPÍTULO CUARTO

Para el empresario, su información, como activo del negocio es básica para mantener la competitividad, rentabilidad, conformidad legal e imagen corporativa. Por ello, antes de migrar la información de la cual depende en mayor o menor medida su continuidad empresarial, será necesario, por una parte, que se asegure de la calidad del servicio que oferta el proveedor con quien contrata, y de las responsabilidades que asume este proveedor en cuanto a la custodia de tales datos. Por otra parte, deberá velar por conservar y mantener los derechos derivados de esta información.

Así, nos encontramos frecuentemente con contratos en los que se otorgan, de forma casi inadvertida para el suscriptor, cesiones de uso y licencias que tienen por objeto datos amparados bajo la normativa de propiedad intelectual[3]. Estas concesiones suelen revertir en favor del proveedor o de sus subproveedores. Igualmente, existen en muchas ocasiones reservas de uso de otros contenidos, como aquellos datos personales aportados para la contratación del servicio, archivos de

---

responsabilidades de las partes del contrato de computación en la nube".

3 Paradigmático resulta el caso de la red social Facebook, que en la versión española de sus condiciones de servicio establece: "Con relación al contenido protegido por derechos de propiedad intelectual, como fotografías y vídeos (...), nos concedes específicamente el siguiente permiso, de acuerdo con la configuración de la privacidad y las aplicaciones: nos concedes una licencia no exclusiva, transferible, con derechos de sublicencia, libre de derechos de autor, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook (...). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta, salvo si el contenido se ha compartido con terceros y estos no lo han eliminado. (...) Cuando publicas contenido o información con la configuración "Público", significa que permites que todos, incluidas las personas que son ajenas a Facebook, accedan y usen dicha información y la asocien a ti (es decir, tu nombre y foto del perfil). Siempre valoramos tus comentarios o sugerencias acerca de Facebook, pero debes entender que podríamos utilizarlos sin obligación de compensarte por ello (del mismo modo que tú no tienes obligación de ofrecerlos)". Estas cláusulas aparecen en las "condiciones de servicio" y no en la página que incluye la "política de datos". Es en esta última donde se enumera la información del usuario recopilada por Facebook ("Recopilamos el contenido y demás información que proporcionas cuando utilizas nuestros servicios, incluido al registrarte para obtener una cuenta, al crear o compartir contenido y cuando envías mensajes o te comunicas con otros usuarios. Esta información puede corresponder a datos incluidos en el contenido que proporcionas o relacionados con él, como el lugar donde se hizo *una foto o la* fecha de creación de un archivo. También recopilamos información sobre el uso que haces de los servicios; por ejemplo, el tipo de contenido que ves o con el que interactúas, o la frecuencia y la duración de tus actividades") y los usos a los cuales se destina ("proporcionar, mejorar y desarrollar los servicios; comunicarnos contigo; mostrar y medir anuncios y servicios; y fomentar la seguridad y la protección"). Aunque Facebook afirma usar los datos del usuario para tales finalidades, no se compromete a ceñirse estrictamente a tales usos. La licencia tan amplia otorgada en las condiciones de uso podría permitirle un acceso y control prácticamente libres a los contenidos publicados por el usuario. Términos legales de Facebook [en línea]. Disponible en: <https://es-es.facebook.com/legal/terms?locale=es_ES> y <https://es-es.facebook.com/about/privacy/>. [Fecha de consulta: 25 de abril de 2017].

diversa índole que el usuario pueda compartir en la nube con otros usuarios, o metadatos que registran la actividad que proviene de cada cuenta de acceso[4]. El proveedor, mediante la inclusión de tales cláusulas, quedaría habilitado para utilizar, de forma más o menos amplia (según sea la letra de las condiciones de adhesión), todos estos contenidos que el cliente y/o usuario final migrará mientras dure la relación contractual.

Estas reservas no suponen ningún obstáculo para que el cliente siga siendo responsable por los contenidos migrados y por las actividades que realiza en el marco del servicio prestado. Para controlar su legalidad y adecuación, se establece contractualmente la llamada política de uso adecuado del servicio, (en adelante, PUA[5]), un pliego de requisitos de comportamiento a los que debe someterse el usuario, y a través del cual muchos proveedores se reservan el acceso a los contenidos y procesos del usuario para vigilar que no se lleve a cabo ninguna de las actividades restringidas. En este mismo capítulo expondremos sus estipulaciones más habituales.

Respecto del cumplimiento de estas políticas de uso, en la práctica es habitual que se atribuya al proveedor la facultad de único órgano decisor, con la facultad de dirimir si efectivamente se ha infringido tal política de uso, y determinar discrecionalmente las consecuencias sobre la relación contractual y sobre la continuidad de la prestación del servicio que tal infracción pueda acarrear, con lo cual el cliente puede, en ocasiones, encontrarse con suspensiones de la prestación y sin posibilidad de acceder a un procedimiento abierto para recuperar el acceso al servicio o, incluso, a sus datos[6].

---

4 Los *metadatos* son datos adjuntos a archivos de documentos, imágenes, vídeos, hojas de cálculo o páginas web, y contienen información sobre su autor, fecha de creación, fecha de modificación, tamaño del archivo, palabras clave, etc. Pueden crearse manualmente o ser generados de forma automática por un programa informático, y resultan esenciales para realizar operaciones de búsqueda, almacenamiento, transferencia o procesamiento de archivos. (Definición propia).

5 Política de uso adecuado o PUA. Conjunto de cláusulas que regula la manera en la que los clientes deben usar del servicio, así como determinadas acciones prohibidas, presente en todos los contratos de suministro de servicios de computación en la nube. (Definición propia). Ver apartado "Legalidad y adecuación de los contenidos alojados por el cliente. Las políticas de uso adecuado y su control por el prestador de servicios", en este mismo capítulo.

6 El presente capítulo abordará el tema de las políticas de uso adecuado y sus contenidos y consecuencias jurídicas, dejando la cuestión del procedimiento interno de suspensión del servicio a

Tras estas cuestiones introductorias, en este capítulo estudiaremos los contenidos más habituales de la políticas de uso adecuado, así como la forma en que se abordan, en los contratos de adhesión, y en nuestro ordenamiento jurídico, los supuestos relacionados con la "propiedad" de los datos (confidenciales, secretos de empresa y/o sujetos a derechos de propiedad intelectual) aportados por el cliente y/o por el usuario final de servicios de computación en la nube[7]. Concretamente, analizaremos cómo se protegen tanto los datos que puedan entregar el cliente y/o el usuario final durante la relación contractual como los contenidos que el proveedor pone a su disposición a través del servicio que suministra.

No podemos empezar este capítulo sin volver a mencionar el trabajo que realiza, en el marco de la Comisión Europea, la *Cloud Computing Strategy*, y más concretamente su grupo de expertos en contratos de computación en la nube. Su intención es crear cláusulas modelo equitativas que, de forma voluntaria, los proveedores de servicios de computación en la nube incorporen en sus contratos de adhesión con consumidores y pequeñas empresas. Sin embargo, y aunque en principio no es esa su finalidad, puede que el fruto de estos debates entre los expertos de la *Cloud Computing Strategy* más adelante se refleje en algunas reformas normativas, dada la importancia económica, jurídica y social de la materia[8]. Asimismo, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) está estudiando la posibilidad de incluir en un futuro texto no normativo sobre contratos de *Cloud Computing* algunas cuestiones sobre propiedad intelectual[9].

---

otro apartado, dedicado a tal efecto, en el capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

7 Como vemos, el tema de los datos dentro de entornos de computación remota es amplio y complejo. Por ello, aplicaremos conceptos de propiedad intelectual, secreto comercial y propiedad industrial de manera instrumental, con el fin de plantear la eventual problemática derivada de los términos contractuales habituales en la suscripción de servicios de computación en la nube, y relacionar esta problemática con la normativa que pueda resultar de aplicación.

8 Los debates del Grupo de Expertos de la *European Cloud Computing Strategy* abarcan diferentes aspectos de la contratación de servicios de computación en la nube, además de la revelación y la integridad de los datos: su localización y transferencia, la propiedad de los datos, la responsabilidad directa e indirecta de los proveedores, la subcontratación de servicios, la conservación de los datos una vez finalizado el contrato, etc. Documentación sobre los debates del grupo de expertos de la *Cloud Computing Strategy* [en línea]. Disponible en: <https://ec.europa.eu/digital-agenda/en/european-cloud-initiative>. [Fecha de consulta: 3 de agosto de 2016].

9 El Grupo de Expertos IV de la CNUDMI se plantea la posibilidad de incluir o no en este texto

2.- CLASIFICACIÓN DE LOS DATOS ALOJADOS EN LA NUBE

En el entorno de la nube coexisten contenidos aportados por los usuarios y contenidos que el propio proveedor pone a disposición de estos como parte de las funcionalidades del servicio. Los contenidos aportados por el usuario pueden ser, atendiendo a su origen: a) contenidos creados por el propio usuario y posteriormente migrados a la nube; b) contenidos creados por el propio usuario gracias a las funcionalidades que permite el entorno *cloud* contratado; c) contenidos creados por terceros y que el usuario sube a la nube para almacenarlos, procesarlos, ejecutarlos, o compartirlos con otros usuarios; y d) datos identificativos del usuario y/o del suscriptor y que permiten su acceso autorizado al servicio (nombre, alias, datos de contacto, profesión, datos bancarios...)[10].

Esta distinción de los datos según su procedencia permitirá aclarar ciertos aspectos relacionados con su titularidad, uso y control por parte de proveedor, usuario y terceros, como estudiaremos en los siguientes apartados. En los contratos raramente se establecen diferencias de régimen jurídico de los datos atendiendo a su origen, sino que son englobados en conceptos más amplios, como "contenidos del usuario", "tus archivos", "datos almacenados", "datos de tu cuenta", "tus datos", etc. En cambio, se suele hacer siempre una especial mención a los "datos de carácter personal", con la finalidad de recabar autorización e informar sobre su tratamiento[11].

---

cuestiones relacionadas con la contratación de *Cloud Computing* y la propiedad intelectual: "Sería necesario aclarar hasta qué punto se deberían analizar cuestiones relacionadas con la propiedad intelectual en un texto de orientación. Algunos expertos se hicieron eco de las opiniones ya expresadas en el sentido de que las cuestiones de propiedad intelectual deberían estar excluidas (véanse los párr. 1 y 2 supra). Otros sugirieron que se destacaran en un texto de orientación los riesgos que entrañaba explotar derechos de propiedad intelectual mediante acuerdos de computación en la nube". Estas cuestiones, de incluirse en el futuro texto, podrían versar sobre: "licencias patentadas versus normas libres; limitaciones a la reproducción de contenidos y a la comunicación al público; derechos sobre aplicaciones que los clientes hayan creado o desplegado en la nube; cuestiones de propiedad intelectual planteadas a raíz de modificaciones de datos de los clientes; derechos de propiedad sobre los datos procesados en la nube (por ejemplo, metadatos); derechos sobre las mejoras derivadas de sugerencias del cliente; otros casos de propiedad intelectual compartida; e interacción entre hechos relacionados con la propiedad intelectual y el deber de diligencia". COMISIÓN DE LAS NACIONES UNIDAS (CNUDMI) GRUPO DE TRABAJO IV, *Aspectos contractuales de la computación en la nube A/CN.9/WG.IV/WP.142* [en línea]. Disponible en: <http://www.uncitral.org/uncitral/es/commission/working_groups/4Electronic_Commerce.html>. [Fecha de consulta: 30 de mayo de 2017].

10 Son los datos que se facilitan al proveedor al dar de alta una cuenta como usuario del servicio.

11 Ver capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

Los contenidos migrados pueden recorrer diferentes trayectos durante el transcurso de la relación contractual:

1.- Los datos del usuario que van a subirse al sistema *cloud* transforman su formato para ser compatibles en el nuevo entorno y se trasmiten desde el dispositivo del usuario hasta el entorno del proveedor a través de una conexión de red (generalmente, Internet).

2.- Estos datos son procesados y almacenados en la nube. Dentro de la nube, probablemente se trasladen y/o repliquen de forma automática en diferentes servidores integrados en centros de procesamiento de datos dispersos geográficamente.

3.- El usuario puede recuperar sus datos descargándolos de nuevo en su dispositivo. A su vez, puede borrarlos (en principio, de forma no definitiva) del entorno[12].

4.- Una vez finalizado el contrato, el proveedor deberá posibilitar la recuperación del total de los datos del cliente que permanecen en su sistema, para posteriormente proceder, con más o menos garantías, a su borrado definitivo.

Por su parte, el proveedor puede poner a disposición del usuario *cloud* los siguientes contenidos, que pueden clasificarse en: a) información sobre el funcionamiento, la seguridad o los aspectos técnicos del entorno *cloud* y del servicio suscrito; b) imágenes, textos, logotipos, marcas, bases de datos, software y otros contenidos de los cuales el proveedor ostenta la titularidad; y c) imágenes, textos, logotipos, marcas, bases de datos, software y otros contenidos titularidad de terceros proveedores.

Para proteger los intereses en materia de propiedad intelectual e industrial que correspondan tanto al proveedor principal (es decir, aquel con quien el cliente suscribe el contrato) como a los eventuales subproveedores del servicio (por ejemplo, proveedores de otro software, como aplicaciones accesorias o antivirus, o de capas subyacentes de la infraestructura de la nube), es habitual encontrar cláusulas

12 Ver apartado "La preservación de los contenidos y su borrado una vez extinguida la relación contractual", en el capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

correspondientes a licencias de uso restringido y prohibiciones sobre infracciones de derechos de propiedad intelectual y realización de ingeniería inversa[13] en las PUA[14].

En cuanto a otras responsabilidades relacionadas con los contenidos migrados, como posteriormente trataremos con más detalle, la mayoría de proveedores excluyen por vía contractual su responsabilidad ante reclamaciones por contenidos lesivos aportados por los usuarios materiales del servicio[15]. Del mismo modo, cuando el suscriptor de los servicios sea un empresario o un profesional y los usuarios finales sus empleados o clientes, el proveedor *cloud* considerará responsable, por lo general, al suscriptor por aquellos usos ilegítimos que los usuarios materiales puedan hacer del servicio[16]. Y así se reflejará en las condiciones generales predispuestas.

Finalmente, los contenidos alojados en la nube, independientemente de si son aportados por el usuario o por el proveedor, pueden tener distinta naturaleza: a) contenidos virtuales que tienen un equivalente en formato físico tradicional[17], b)

13 Ingeniería inversa. Obtención de información sobre los componentes de fabricación y el mecanismo de funcionamiento de un producto físico o de un programa informático a través de un examen directo del producto o del dispositivo que contiene el programa cuando se obtiene o se usa de forma legal. (Definición propia).

14 El proveedor Google establece unas condiciones comunes para todos sus servicios *(Gmail, Youtube, Buscador Google, Google Maps*, etc.) [en línea]. En ellas, se concede esta licencia a sus usuarios: "Google te concede una licencia personal mundial, libre de *royalties*, intransmisible y no exclusiva para usar el software que se te proporcione como parte de los servicios. El único propósito de esta licencia es permitirte usar los servicios que ofrece Google y beneficiarte de ellos, según lo estipulado en estas condiciones. No podrás copiar, modificar, distribuir, vender ni prestar ninguna parte de nuestros servicios ni del software incluido ni podrás aplicar técnicas de ingeniería inversa ni intentar extraer el código fuente de dicho software, salvo si la legislación prohíbe dichas restricciones o si tienes consentimiento de Google por escrito". Disponible en: <http://www.google.com/policies/terms/>. [Fecha de consulta: 25 de abril de 2017].

15 Ver apartado "Legalidad y adecuación de los contenidos alojados por el usuario. Las políticas de uso adecuado y su control por el prestador de servicios", en este mismo capítulo, y el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

16 Por ejemplo, esta obligación del cliente suscriptor del software como servicio de almacenamiento (SaaS) *Dropbox para empresas*, que aparece recogida en sus condiciones generales [en línea]: "El cliente es responsable del uso de estos servicios por parte de los usuarios finales. El cliente y sus usuarios finales deben usar los servicios de conformidad con la política de uso aceptable (…)". Disponible en: *<https://www.dropbox.com/privacy#business_agreement>.* [Fecha de consulta: 3 de agosto de 2016].

17 Contenidos virtuales que tienen un equivalente en formato físico. Son unidades lógicas que permiten el almacenamiento digital de contenidos tradicionalmente expresados en soportes físicos como papel o cintas. Forman parte del global de archivos informáticos definidos por formatos estándar (.ODT, .DOC, .PDF, .XLS, .JPG, .MP3, .PNG, .MOV, .AVI, etc.). [Estos formatos

bases de datos[18], c) programas informáticos[19], d) metadatos; y f) datos derivados de la actividad de los usuarios[20].

Asimismo, la materia objeto de estos contenidos (datos personales, actividades del usuario del sistema, información empresarial, obras artísticas o científicas, etc.) es relevante jurídicamente, puesto que nos ayudará a determinar la normativa que puede ser de aplicación (protección de datos, deber de confidencialidad, secreto de empresa, propiedad intelectual, etc.) a efectos de protegerla jurídicamente contra accesos o usos de terceros no autorizados por su titular, como veremos en posteriores apartados de este capítulo.

A continuación, analizaremos algunos aspectos relacionados con la política de uso adecuado o PUA.

3.- LEGALIDAD Y ADECUACIÓN DE LOS CONTENIDOS ALOJADOS POR EL USUARIO. LAS POLÍTICAS DE USO ADECUADO Y SU CONTROL POR EL PRESTADOR DE SERVICIOS

En capítulos anteriores hemos observado las posibilidades que ofrece para empresas y particulares el uso de la tecnología en la nube. Uno de sus problemas

---

corresponden a: archivos de texto (*.ODT, .DOC, .PDF*), hojas de cálculo (*XLS*), imagen (*.JPG*), sonido (.mp3) y vídeo (*.PNG, .MOV, .AVI*)]. Dependiendo del servicio en la nube, se permitirá crearlos (en línea u *offline)*, procesarlos, ordenarlos en ficheros, publicarlos en la Red y compartirlos con otros usuarios, almacenarlos en servidores remotos, etc. (Definición propia).

18 Bases de datos. Conjuntos de datos relacionados, creados con lenguajes informáticos especiales (*SQL, XQuery,* etc.) organizados para soportar procesos de búsqueda, captura y análisis de información. Se administran a través de aplicaciones software específicas, también conocidas como *DBMS* o *Database Managed Systems* (*MySQL, Oracle*, etc.), y son aplicables a cualquier sector empresarial, desde banca (información de clientes, cuentas y otras transacciones bancarias) hasta universidades (informaciones de y para el alumno, acceso a documentos de bibliotecas y catálogos o a información académica, etc.) o factorías (administración de las cadenas de montaje, rastreo de productos, inventarios en *stock* y distribuidores, etc.). (Definición propia).

19 Programas informáticos. Conjunto de instrucciones lógicas y reglas informáticas que permiten ejecutar tareas y operaciones dentro de un entorno de computación. (Definición propia).

20 Datos derivados de la actividad de los usuarios. Conjunto de información extractada de patrones procedentes del análisis combinado de múltiples bases de datos, que contiene información sobre actividades de los usuarios, con su propio valor comercial, y capaces de predecir cambios de comportamientos en los consumidores, votantes, etc. Estos sistemas de extracción se conocen como "minería de datos" (*data mining*). (Definición propia). Ver apartado "Datos generados por el proveedor o por terceros a partir de la información de los usuarios", en este mismo capítulo.

radica en que no todos los usuarios pretenden aprovechar las funcionalidades de los servicios *cloud* para fines lícitos. El proveedor exigirá, como requisito previo al acceso a sus sistemas de información, a la migración de datos y al uso de sus aplicaciones, que el suscriptor adquiera un compromiso de buen uso del servicio. A continuación, analizaremos este tipo de compromisos.

3.1.- Las PUA en los contratos de computación en la nube

Estos compromisos, llamados políticas de uso aceptable o *Acceptable Use Policies* (en adelante, también PUA), pueden definirse como la cláusula o conjunto de cláusulas que regulan la manera en la que los clientes deben usar el servicio, así como determinadas acciones prohibidas.

Estas cláusulas están presentes en la gran mayoría de contratos de prestación de servicios de computación en la nube. Este tipo de políticas no se limitan a las condiciones generales de servicios en la nube, sino que se utilizan en otros muchos contratos de bienes y servicios tecnológicos, como los servicios de telecomunicaciones o las páginas web[21].

21 La empresa Vodafone distingue entre sus políticas de uso de comunicaciones electrónicas para particulares y autónomos ("Para garantizar el buen uso de los servicios de comunicaciones electrónicas de Vodafone, serán aplicables las siguientes normas de uso razonable, cuyo incumplimiento por parte del cliente (..) facultará a Vodafone, previo aviso al cliente, a excluirle, de forma automática, de la tarifa o promoción comercial contratada y/o restringirle el acceso a futuras promociones comerciales de Vodafone y/o, en su caso, resolver con carácter automático las condiciones generales (…). Dichas normas de uso razonable son, a título anunciativo y no limitativo, las siguientes: 1. Los servicios de comunicaciones electrónicas de Vodafone son incompatibles con la realización de llamadas o envío de SMS cuyo origen y destino no sea directamente usuarios finales (…). 2. Queda prohibido el uso spam, mensajes (sms, mms, etc) enviados de forma masiva que perjudiquen a otros usuarios. 3. Queda prohibido el uso intensivo y continuado que pueda provocar o provoque congestión en la red Vodafone (…). 4. Se prohíbe la realización de su uso anómalo y/o desmesurado de los servicios") y las políticas de uso para empresas ("El cliente se compromete a (I) hacer un uso lícito del servicio no perjudicando derechos de terceros, (II) no obtener un beneficio económico por la utilización del servicio distinto del derivado de este contrato, ni utilizar su condición de cliente para llevar a cabo una actividad empresarial, profesional o económica cuyo objeto sea revender el servicio prestado por Vodafone o explotar el servicio para otros fines en cualquier forma. El incumplimiento o la apreciación objetiva, por parte de Vodafone, del riesgo de incumplimiento de las obligaciones anteriormente citadas, permitirá a Vodafone proceder a la resolución automática del contrato. Dichas normas de uso razonable son, a título enunciativo y no limitativo, las siguientes: 1.Se excluye expresamente la utilización de la tarjeta sim como Sim-box o enrutador masivo de llamadas (…). 2. Queda excluido el uso spam (...). 3. Queda excluido el uso masivo a destinos de tarificación especial, de voz, datos y sms"). Como ejemplo de una PUA en una página web, la disponible en la tienda *online* de aspiradoras y otros electrodomésticos Dyson ("Estos términos de uso, junto con el resto de documentos a los que se hace referencia, contienen los términos en los que podrá hacer uso de nuestra página *www.dyson.es*, ya sea como visitante o como usuario registrado. El uso de la web

Además, debe prestarse atención a otras restricciones de uso que, a pesar de no estar incluidas como condiciones generales del contrato, puedan ser vinculantes para el cliente, como las que se incluyen en otras ubicaciones dentro del sitio web (por ejemplo, en las fases del proceso de registro como usuario o en hipervínculos)[22]. Aunque estas cláusulas estén dispersas, se entiende que forman parte de las políticas de uso adecuado, con lo cual será importante que estén accesibles, que no se oculten al cliente o que no le puedan pasar inadvertidas, pues forman parte de los compromisos contractuales que suscribe al contratar el servicio, como parte de la información sobre el servicio que ofrece el proveedor.

Las PUA cumplen diversas funciones: informan al cliente de los usos permitidos y prohibidos del servicio (con lo cual deben estar redactadas en forma clara e inteligible para el usuario final a quien, en su caso, el cliente debe informar también); delimitan la responsabilidad del proveedor, del cliente y del usuario final en relación a las actividades prohibidas; y establecen posibles consecuencias de comportamientos ilícitos por parte de los usuarios finales.

Por su parte, la Ley 34/2002 de Servicios de la Sociedad de la Información (apartado 4 de su art. 12 bis) también obliga, aunque solo a los proveedores de servicios de acceso a Internet, a facilitar información a sus clientes "acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial"; esta obligación se entiende cumplida si se publica la PUA en la página web del proveedor. Generalmente, en esta se habilitan los enlaces al contrato de adhesión que suelen incluir las actividades restringidas e ilícitas en su articulado o en sus anexos (apartado 5 del art 12 bis.[23]). En caso de que no sea así, se considera infracción administrativa leve (art. 38.4.a) por la propia LSSI. En nuestra opinión, sería

incluye el acceso, la navegación o el registro para el uso de nuestra web. [...]. Al usar nuestro sitio web, confirma que acepta estos términos de uso y se compromete a cumplirlos. Si no está de acuerdo con estos términos, no use nuestra web"). Políticas de Uso Adecuado disponibles respectivamente en: <http://www.vodafone.es/conocenos/es/vodafone-espana/quienes-somos/legal-y-regulatorio/politica-de-uso/> y <http://www.dyson.es/soporte/terminos-de-uso-y-politica-de-uso-aceptable.aspx>. [Fecha de consulta: 25 de abril de 2017].

22 BRADSHAW, S; MILLARD, C; WALDEN, I, "Standard contracts for Cloud Services", *Cloud Computing Law,* (Coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 67.

23 Apartado 5 del artículo 12 bis de la LSSI: "Las obligaciones de información referidas en los apartados anteriores se darán por cumplidas si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet en la forma establecida en los mencionados apartados".

razonable proponer la aplicación analógica de esta obligación de información a los proveedores de servicios de computación en la nube, con el fin de obtener una mayor transparencia entre las partes.

A pesar de la heterogeneidad de los servicios *cloud* ofrecidos, las PUA analizadas de los distintos proveedores de nube pública comprenden similares previsiones y efectos, aunque pueden variar en su extensión y en el detalle con el que se recogen los comportamientos no tolerados[24]. A continuación, exponemos un compendio de los usos ilícitos o impropios generalmente recogidos por los proveedores de servicios *cloud* en las PUA[25]:

a) Actividades ilegales: infracciones de derechos de autor o marcas registradas de terceros, fraude, tráfico de material obsceno, etc.

b) Alojamiento de contenidos ofensivos, obscenos, difamatorios, intimidatorios o que inciten al odio o a la violencia, etc.

c) Desarrollo, instalación o ejecución de software dañino: virus y demás software malicioso, recopilación de contenidos o datos de otros usuarios a través de medios técnicos, etc.

d) Uso abusivo de los recursos (espacio de almacenamiento excesivo, uso de programas que puedan saturar, bloquear o dañar el entorno o la Red...) o acciones que puedan interferir, entorpecer o dificultar el suministro del servicio a otros usuarios del sistema; promoción de comunicaciones o publicaciones comerciales masivas no autorizadas por el proveedor (*mail bombing*[26] o *spamming*[27]), etc.

---

24 En el mismo sentido, BRADSHAW, S; MILLARD, C; WALDEN, I, *op. cit.*, pág. 67.

25 Por motivos de extensión, hemos considerado más acertado incluir varios enlaces de ejemplos de PUA, en vez de adjuntarlos en el cuerpo de texto. A tal efecto, adjuntamos a continuación los enlaces de las políticas publicadas por los proveedores Amazon (concretamente, de su servicio *Amazon Drive*), Apple (de su producto *iCloud*, en el apartado V. B: Conducta) y Twitter (en el apartado "restricciones en el contenido y uso de los servicios"). Disponibles respectivamente en: <https://www.amazon.es/gp/help/customer/display.html?nodeId=201376540ref_=cd_home_tou>, <https://www.apple.com/legal/internet-services/icloud/es/terms.html> y <http://www.twitterenespanol.net/terms_of_use.php>. [Fecha de consulta: 25 de abril de 2017].

26 *Mailbombing* o "bombardeo postal". Acto de enviar, a menudo a través de programas informáticos creados a tal efecto, grandes cantidades de mensajes electrónicos con la finalidad de saturar el sistema o la bandeja de entrada de un usuario. (Definición propia).

27 *Spamming o "*correo basura". Envío masivo, a través del correo electrónico u otro tipo de

e) Violaciones de seguridad del sistema: acceso a cuentas de otros usuarios sin autorización, alteración o destrucción o lesión de datos de otros usuarios, uso de datos personales de terceros sin su consentimiento, monitorizaciones del sistema sin consentimiento, pruebas de detección de vulnerabilidades del sistema no autorizadas, etc.

f) Falsificación de datos: facilitar datos personales o de pago no veraces, etc.

g) Otras restricciones para salvaguardar intereses legítimos de proveedores y terceros, como la prohibición de realizar actos de ingeniería inversa.

Por supuesto, atendiendo a la categoría de servicio y a otras motivaciones del proveedor, pueden establecerse usos restringidos adicionales[28]. Del mismo modo, es frecuente que se admita en la misma PUA que la lista de actividades y contenidos recogidos es una lista orientativa y abierta, lo cual facilita al proveedor un margen aún más amplio de actuación.

Para controlar las eventuales infracciones de las actividades restringidas, es habitual que el proveedor monitorice la actividad del cliente y/o usuario, aunque no

---

mensajería móvil o en línea, de anuncios publicitarios no solicitados que no permiten identificar la dirección de correo verdadera del remitente. (Definición propia)

28 Algunos proveedores, como ElasticHost, suministrador de servicios *cloud* de infraestructura, no permiten a sus usuarios el uso de servicios en sistemas críticos de seguridad ("*safety-critical*") en los que un fallo en el servicio pueda suponer grave peligro o desencadenar pérdidas de vidas humanas o daños a otros bienes de interés general, como el medio ambiente. Quedarían excluidas de poder usar estos servicios empresas que pretendan sustentar en este servicio *cloud* los controles de manejo de armas masivas en desarrollo o de sistemas de pilotaje automático de aviación, por ejemplo. Así lo establece en sus condiciones generales de contratación [en línea]. <http://www.elastichosts.com/cloud-servers/terms-of-service/> [Fecha de consulta: 12 de agosto de 2016]. Otras restricciones de uso pueden deberse a razones de índole política. Por ejemplo, el proveedor *cloud* ADrive no permite a residentes en países sometidos a embargos o sanciones económicas por EEUU el uso de su servicio de almacenamiento remoto ("No Storage Data shall be acquired by or otherwise exported or re-exported into (or by or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Syria, Sudan or any other country to which the U.S. has embargoed goods; or to anyone on the U.S. Treasury Department's list of Specially Designated Nationals and Blocked Persons or the U.S. Commerce Department's Table of Denial Orders. As a Storage Data Recipient and/or User, You represent and warrant that You are not located in, under the control of, or a national or resident of any such country or on any such list"). Términos que, por otra parte, no han sido modificados tras el restablecimiento de las relaciones diplomáticas entre Estados Unidos y Cuba. Términos contractuales de ADrive [en línea]. Disponible en: <http://www.adrive.com/terms>. [Fecha de consulta: 25 de abril de 2017].

siempre lo mencione en las condiciones generales[29]. Cuando sí se refleja por escrito, el contrato reconoce la finalidad de estas monitorizaciones, a menudo obligado por la legislación sobre privacidad[30]. El proveedor frecuentemente afirma limitarse a controlar la calidad del servicio, y/o el cumplimiento de la PUA a través del acceso puntual a los datos almacenados o al registro de actividades.

Los servicios *cloud* de infraestructura y plataforma, al ofrecer la capacidad informática suficiente para desarrollar e implementar herramientas lógicas, proporcionan el marco adecuado para la creación de software malicioso y que el servicio se use activamente para actividades delictivas, con lo cual la monitorización tendría que ir más allá de la comprobación de los contenidos alojados que pueda efectuar un proveedor de un servicio *cloud* de software[31]. Sin embargo, y en especial en los servicios de infraestructura, el tratamiento que los proveedores realizan del servicio es de una especie de "paquete blindado" (máquinas virtuales y aplicaciones de programación o API que permiten su ejecución directamente desde el servidor de los clientes, sobre la infraestructura del proveedor), con lo cual el proveedor suele permanecer desconocedor sobre las aplicaciones que despliega el cliente en el entorno de nube[32].

Otra manera de controlar las infracciones de las PUA es a través de la comunidad de usuarios[33]. A menudo, en el propio sitio web del proveedor se facilitan

29 La monitorización se realiza a través de software diseñado a tal efecto con diferentes fines, por ejemplo para controlar el rendimiento del servicio o las medidas de seguridad instaladas, o para obtener datos sobre las actividades de los usuarios. En cuanto a este último aspecto, la información que pueden aportar estas herramientas es variada (uso de recursos, detección de niveles anormales de actividad, etc.), aunque la fundamental radica en los tiempos de conexión de los usuarios al servidor y los comandos ejecutados en cada una de las sesiones.

30 Ver capítulo "Privacidad en la nube. Principales cuestiones sobre protección de datos de carácter personal".

31 BRADSHAW, S; MILLARD, C; WALDEN, I, *op. cit.*, pág. 67.

32 ENISA, *Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información* [en línea], 2009. Disponible en: <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish>. [Fecha de consulta: 25 de abril de 2017].

33 Según DE MIGUEL ASENSIO, "la puesta a disposición de mecanismos voluntarios de detección y retirada por parte de los prestadores de servicios de alojamiento (...) constituye una buena práctica que de be ser fomentada, en la medida que se facilita un cauce específico de comunicación con el prestador de servicios de alojamiento para la denuncia de la presencia de contenidos ilícitos(...). Aunque la adopción de un cauce de comunicación como este va unido aparentemente a ciertos riesgos -en la medida en que facilita que el proveedor pase a ser responsable por los contenidos- e implica costes -asociados a la gestión de las

protocolos a disposición de aquellos usuarios que quieran denunciar conductas poco apropiadas de otros usuarios de las cuales hayan tenido conocimiento. Este mecanismo se utiliza frecuentemente en redes sociales.

Por añadidura, y considerando la PUA como un contenido más del contrato, el proveedor, a través de la reserva del derecho de modificación unilateral del contrato, puede enmendar la PUA y ampliar las actividades inicialmente restringidas, como reflejo de actualizaciones legislativas o de cambios en su política comercial[34]. Si el usuario no tiene conocimiento efectivo de estos cambios, y puesto que se suele establecer contractualmente que la continuación en el uso del servicio implica la aceptación tácita de modificaciones de las condiciones del servicio, puede encontrarse realizando actividades que en un primer momento eran aceptables y que pasan a estar prohibidas[35].

Aunque el particular puede verse perjudicado por el cierre de su cuenta como usuario del servicio, las consecuencias del incumplimiento de las PUA resultan especialmente graves en cuanto a continuidad operativa cuando el cliente es un empresario o profesional. La imputación de la infracción queda sometida generalmente al único arbitrio del proveedor, quien decidirá discrecionalmente sobre las consecuencias del incumplimiento del acuerdo sobre el uso del servicio y, eventualmente, sobre la adopción de medidas cautelares mientras se investigan los hechos y se identifica al autor (medidas que pueden afectar al resto de usuarios finales del servicio contratado por la entidad suscriptora).

La posición decisoria del proveedor que le permite, en caso de infracción de la PUA, acordar la suspensión del servicio para el usuario o cliente (con o sin previo aviso, dependiendo de lo estipulado), la retención de sus datos, la denuncia a las autoridades o la determinación de indemnizaciones por daños y perjuicios, debería, a

---

reclamaciones recibidas-, es evidente que se trata de una práctica beneficiosa que es muestra de la diligencia del prestador de servicios, lo que precisamente favorece que pueda beneficiarse de la exención". DE MIGUEL ASENSIO, Pedro A., *Derecho privado de Internet*, Navarra, 2011, pág. 252.

34 Respecto de la modificación unilateral de efectuada por el proveedor del servicio *cloud*, consideramos que el proveedor debe notificar al suscriptor de los servicios de los cambios relevantes que puedan sufrir las cláusulas o la prestación. Para mayor detalle, nos remitimos al apartado "La modificación unilateral de cláusulas contractuales", en el capítulo "Modificación, suspensión y extinción del contrato de computación en la nube".

35 BRADSHAW, S; MILLARD, C; WALDEN, I, *op. cit.*, pág. 64.

nuestro parecer, acotarse mediante un procedimiento más equitativo, informado y abierto, en el cual se permitiese efectuar alegaciones al usuario, y existiera una efectiva proporcionalidad en la adopción de tales medidas provisionales y sus consecuencias.

Por añadidura, el proveedor, en muchas ocasiones, tampoco garantiza preaviso ni información sobre decisiones o sanciones por incumplimiento de la PUA, con lo cual el usuario puede verse ante una situación de total desconocimiento de las causas que motiven la suspensión del servicio, y su consecuente desamparo[36]. Para preservar los derechos de defensa de los usuarios y clientes, es prudente que el proveedor se asegure de que aquellos reciben alertas por escrito no solo sobre infracciones de PUA, sino también sobre otros eventuales incumplimientos contractuales (por ejemplo, falta de pago de cuotas de suscripción) y sobre las modificaciones que, unilateralmente, pueda sufrir el acuerdo contractual una vez formalizado. Especialmente cuando tengan lugar cambios que afecten a las PUA, consideramos fundamental el trámite de información activa por parte del proveedor *cloud*, más efectivo que la tarea delegada al cliente de comprobación periódica de las actualizaciones publicadas *online.*

En los procesos internos sancionadores arriba mencionados, las consecuencias legales no recae siempre sobre el usuario final de forma directa, sino que el suscriptor profesional, como adherente, se responsabiliza por ellas ante el proveedor, porque generalmente así se ha establecido en los términos contractuales.

En este caso, el usuario final deberá responder ante la empresa suscriptora del servicio *cloud* por aquellos daños y perjuicios a los que esta haya tenido que hacer frente debido a la mala praxis de aquel en el uso del servicio. Así lo deberían recoger los contratos que vinculan a empresa suscriptora y usuario final y que le permiten a este el uso de los servicios en la nube contratados por la primera, para facilitar cualquier reclamación posterior.

36 Ver apartado "La modificación de cláusulas contractuales", en el capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

3.2.- La LSSI y la responsabilidad de los prestadores de servicios en la nube por contenidos alojados

Como hemos visto, son los usuarios finales del servicio quienes, con su comportamiento, pueden incumplir las políticas sobre uso aceptable del servicio. Por tanto, tiene lógica que sean estos (o, en su caso, los empresarios o profesionales que suscriben el servicio), quienes asuman las consecuencias de su infracción[37]. Esto no obsta para que la legislación, en ciertos casos, considere responsables a los proveedores por contenidos creados por terceros y guardados en sus sistemas[38].

En capítulos anteriores[39] hemos considerado al prestador de servicios *cloud* como un prestador de servicios de intermediación a tenor de lo establecido en la LSSI[40]. Esta ley, pretendiendo dotar de mayor seguridad jurídica a los casos en los que se publican contenidos ilegales en Internet, exige a los operadores *online* el deber de colaborar con las autoridades públicas para bloquear el acceso a los contenidos ilícitos y/o retirarlos de la Red[41]. Por ello, esta obligación de colaboración

37 Lo mismo sucederá si es particular, pero contrata en nombre de un menor que será el usuario final.

38 MARTÍNEZ-ROJAS, Ángela, "El deber de diligencia de los prestadores de servicios de intermediación en la sociedad de la información", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 26, 2011, págs. 87 a 100.

39 Ver apartado "El proveedor de servicios en la nube como prestador de servicios de la sociedad de la información", en el capítulo "Elementos subjetivos del contrato de servicios de computación en la nube".

40 Como consecuencia, le serán aplicables los arts. 11 (deber de colaboración de los prestadores de servicios de intermediación) y 16 (responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos) de la LSSI.

41 Art. 11 LSSI: Deber de colaboración de los prestadores de servicios de intermediación. "1. Cuando un órgano competente hubiera ordenado, en ejercicio de las competencias que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación, dicho órgano podrá ordenar a los citados prestadores que suspendan el correspondiente servicio de intermediación utilizado para la provisión del servicio de la sociedad de la información o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente. 2. (...) 3. En la adopción y cumplimiento de las medidas a que se refieren los apartados anteriores, se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información, cuando estos pudieran resultar afectados. (...). 4. Las medidas a que hace referencia este artículo serán objetivas, proporcionadas y no discriminatorias, y se adoptarán de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda". Ver también LLANEZA GONZÁLEZ, *Aplicación práctica de la LSSI-CE,* 1ª Edición, Barcelona, 2003,

es extensible a los proveedores de computación en la nube sometidos al ámbito territorial de aplicación de la LSSI, con lo cual, según el artículo 11, el proveedor puede verse compelido a la suspensión del servicio y/o a la retirada de los contenidos ilícitos publicados.

Uno de los problemas habituales suele consistir en la identificación del usuario final infractor, problema cuya dificultad dependerá mucho del tipo de servicio. En el caso de ciertos servicios, sobre todo en aquellos sujetos a contraprestación económica, podrá ser más fácil localizar al usuario, puesto que a menudo se tratará o bien del obligado a responder por el pago, o bien de un usuario vinculado a la empresa u organización suscriptora. Contrariamente, en ciertos software como servicio y de redes sociales que se ofrezcan gratuitamente, el rastreo puede complicarse, puesto que nada impide en la práctica que un usuario falsee los datos de su suscripción y abra una o varias cuentas con distintas identidades, ya sea con la intención de mantener sus datos personales en el anonimato, ya sea con la intención de realizar actividades ilícitas[42].

Además de este deber de diligencia en cuanto a la retirada de contenidos y de la suspensión del servicio derivados de su artículo 11, la LSSI establece en su artículo 16 la responsabilidad del proveedor de servicios de almacenamiento de datos (uno de los servicios de *Cloud Computing* más extendidos) de retirar o impedir el acceso a datos ilegales (art. 16) de los cuales haya tenido conocimiento efectivo y sepa de su ilicitud o lesividad[43]. Según este artículo, en caso de que el proveedor *cloud* no haya

---

pág. 77.

42 Como señala MARTINEZ-ROJAS en cuanto a la responsabilidad por contenidos ilícitos en blogs, foros y webs que permiten comentarios de los usuarios, algunos de los problemas materiales que se presentan a la hora de perseguir contenidos ilícitos y determinar al responsable de tales contenidos y su difusión son: la ubicación fuera del territorio nacional, el anonimato en la Red, la relativa garantía de que el número IP revele la verdadera identidad del autor del contenido o la difusión colaborativa de contenidos en la web 2.0. En nuestra opinión, estos casos de alojamiento de contenidos son asimilables al alojamiento de contenidos en ciertos software como servicio que permiten la compartición de contenidos entre los usuarios, así como a las redes sociales. MARTÍNEZ-ROJAS, Ángela, *op. cit.,* págs. 88-89.

43 Art. 16 LSSI: "Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que: a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos."

podido tener conocimiento de la existencia de tales contenidos del cliente o de su lesividad o ilegalidad, o cuando haya tenido tal conocimiento efectivo pero ha procedido de manera diligente e inmediata a retirar esos contenidos o hacerlos inaccesibles por otros usuarios, quedará exento de responder por tales contenidos.

Del artículo 16 de la LSSI no se deriva para el proveedor *cloud* la obligación de supervisión de datos ni la realización de búsquedas activas o indagación en datos migrados por los clientes[44] para localizar contenidos ilegales (por ejemplo, descargas de contenidos protegidos por derechos de propiedad intelectual, pornografía infantil o preparación de actos terroristas)[45]. En primer lugar, porque resultaría una tarea especialmente gravosa tanto técnica como económicamente, especialmente para el proveedor *cloud*, teniendo en cuenta el uso masivo y el volumen de migración de datos de la mayoría de servicios[46]. En segundo lugar, por la colisión de esta obligación con otros derechos legítimos de los usuarios finales, como la intimidad personal y familiar, el secreto de las comunicaciones o la libertad de expresión e información[47].

Sin embargo, recordemos que su artículo 11 establece el deber de colaboración a instancia de las autoridades y la obligación de responder en aquellos casos en los cuales no haya actuado con la suficiente diligencia a la hora de retirar o bloquear el acceso a tales contenidos. Aquí se pone de manifiesto la importancia de determinar el alcance de lo que se entiende como conocimiento efectivo de la ilicitud o lesividad de contenidos en el marco de los servicios de computación en la nube.

Nuestra posición coincide con las conclusiones que, a tal efecto, recoge

---

44 El art. 15.1 de la Directiva 2000/31 (Directiva sobre el comercio electrónico) recoge expresamente la inexistencia de este deber general de supervisión: "Los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas respecto de los servicios contemplados en los artículos 12 [mera transmisión], 13 [memoria caché]y 14 [alojamiento de datos]".

45 LLANEZA GONZÁLEZ, A*plicación práctica..., op. cit.*, pág. 91.

46 Así lo consideramos, de acuerdo con la interpretación de la Directiva de Comercio Electrónico, y coincidiendo con del autor BUSTO LAGO, J.M., "La responsabilidad civil de los prestadores de servicios de la sociedad de la información (ISPs)", *Tratado de Responsabilidad Civil, Tomo II* (Coord. Reglero Campos), Navarra, 2008, pág. 1003.

47 LLANEZA GONZÁLEZ, A*plicación práctica..., op. cit.*, pág. 91.

CAVANILLAS respecto de los servidores de alojamiento de datos[48], en las que afirma que, si bien no puede exigírsele al proveedor de servicios de intermediación la supervisión de contenidos de datos alojados, ni siquiera aunque haya podido recibir un aviso de la existencia de tales materiales por un tercero interesado[49], cuando existan mecanismos técnicos gracias a los cuales pudiera probarse que el proveedor ha tenido conocimiento directo de la existencia de estos datos, y que "los ha visualizado y analizado", podría considerarse que ha tenido conocimiento efectivo[50].

48 PAYERAS, Magdalena; CAVANILLAS, Santiago, "Los servidores de acceso y alojamiento: descripción técnica y legal", en *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar*, (Coord. Santiago Cavanillas), 1ª edición, Granada, 2005, págs. 43, 44.

49 Este tercer interesado podría ser otro usuario del servicio de computación en la nube. Como hemos mencionado en otras ocasiones, el proveedor puede incorporar mecanismos para recibir avisos directos, a disposición de otros usuarios o terceros que puedan tener conocimiento de contenidos ilícitos dentro del sistema *cloud*. Incluso en ciertas ocasiones, como hemos visto, estos avisos se han configurado como una obligación contractual para los suscriptores.

50 El concepto de "conocimiento efectivo" que puedan tener los prestadores del servicio de alojamiento de datos de la ilicitud del contenido o actividad aparece en el último párrafo del art. 16.1 de la LSSI: "Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse". Apunta LLANEZA GONZÁLEZ (*Aplicación práctica..., op. cit.,* pág. 92) que no se exige firmeza en la resolución y que el proveedor no tiene porqué ser notificado de tales resoluciones, con lo cual los medios por los cuales el proveedor obtenga conocimiento de la ilicitud de las actividades de su cliente es cuando menos, poco transparente en la LSSI. De todos modos, si existe una resolución administrativa o judicial, el proveedor quedará obligado a informar a las autoridades y a una actuación cautelar de retirada y bloqueo de contenidos. Si, en cambio, lo que tiene son indicios de una potencial lesión de derechos, como la denuncia por otros usuarios, la interpretación amplia que hace del concepto "conocimiento efectivo" la resolución de una de las preguntas frecuentes del sitio web oficial de la LSSI puesto a disposición general por el Ministerio le obliga a actuar incluso ante "sospechas de delito". No obstante, esta interpretación extensiva también opera en casos de infracciones no penales, a tenor del carácter general del art. 13 de la LSSI. Disponible en: <http://www.lssi.gob.es/la-ley/Paginas/preguntas-frecuentes.aspx#dt5> [en línea]. [Fecha de consulta: 15 de junio de 2015]. PEGUERA POCH, por su parte, considera que es voluntad del legislador "limitar las vías por las que el prestador podrá obtener un conocimiento (...) que le obligue a tomas las medidas de pronta retirada, para no perder la exención de responsabilidad", pero afirma que "es claro que no se ha establecido una lista cerrada". Ahora bien, afirma el autor que, ante una demanda presentada contra un prestador de servicios de alojamiento, "el juez deberá apreciar, a la vista de la prueba aportada, si el prestador tuvo o no conocimiento de la ilicitud de la información" y que "no hay obstáculo para que considere probado aquel extremo por cualquier medio de prueba admitido en Derecho, aunque no se haya obtenido el conocimiento a través de los medios recogidos en el art. 16 LSSI". PEGUERA POCH, Miguel, "La exención de responsabilidad civil por contenidos ajenos en

Aún así, como apunta el autor, podría defenderse la postura de que el legislador no ha querido exigir al proveedor la obligación de decidir sobre la difusión o retirada de los contenidos alojados por su cliente, en especial de aquellos contenidos cuya ilicitud no sea claramente manifiesta, con el fin de que pueda ejercerse en Internet la libertad de información y expresión sin injerencias[51].

Tengamos en cuenta que, en muchos de los servicios que suelen implicar el almacenamiento remoto de información, el acceso a los contenidos del usuario no es público, como sucede con los sitios web, sino restringido al suscriptor del servicio o a ciertos usuarios autorizados[52]. Además, teniendo en cuenta las cláusulas sobre suspensión del servicio y monitorización de servicios para controlar el cumplimiento de las PUA (examinadas en otros capítulos[53]), sucederá, como se refleja en ciertos contratos, que en la práctica el proveedor podrá prevenir a su cliente sobre el uso ilegítimo o inapropiado del servicio y sobre la ilegalidad de los contenidos antes de, si así lo decide, adoptar medidas cautelares mientras realiza una investigación interna de los hechos infractores o dar cuenta a las autoridades[54]. Del mismo modo, y también a su libre discreción y conforme a lo establecido en el contrato, el proveedor podrá suspender directamente la prestación del servicio al usuario, o retirar sus

---

Internet"*, Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet* (Coord. Fermín Morales, Óscar Prats), Navarra, 2002, págs. 48 a 49.

51 DE MIGUEL ASENSIO, al respecto, afirma: "no resulta acorde con la posición y los medios de que disponen los prestadores de servicios de alojamiento considerar que a ellos corresponde la tarea de decidir si son ilícitos los contenidos proporcionados por los usuarios de sus servicios, lo que en ocasiones puede requerir un complejo análisis jurídico incluso del alcance y los límites de diversos derechos fundamentales, como la libertad de expresión y el derecho al honor, al tiempo que la respuesta acerca de la licitud o ilicitud de los contenidos puede variar decisivamente en los diversos territorios en que se difunden". DE MIGUEL ASENSIO, Pedro A., *Derecho privado de Internet*, Navarra, 2011, pág. 254.

52 La LSSI distingue, en las responsabilidades de los intermediarios entre aquellos proveedores cuyo servicio consiste en la mera transmisión de datos (como proveedores de acceso a Internet), a los que realizan copias temporales exigidas por la propia transmisión, y los que almacenan datos en sus sistemas. Aunque, como hemos visto en anteriores capítulos, la naturaleza de los servicios *cloud* va más allá del almacenamiento, es con esta última modalidad con la que presenta mayor similitud. Coincidiendo con la opinión de GARCIA MEIXIA, consideramos que sería conveniente que el legislador europeo y español previese un régimen específico más acorde con la naturaleza de la computación en la nube y la asunción por el proveedor de mayores responsabilidades. GARCIA MEIXIA, Pablo, "Cloud Computing. Sus implicaciones legales", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 23, 2010, págs. 79 a 88.

53 Ver apartado "La suspensión del contrato", en el capítulo "Modificación, suspensión y extinción del contrato de computación en la nube".

54 Si bien no será el común de los casos, especialmente cuando se trate de clientes poco relevantes comercialmente, como sucede con los pequeños empresarios.

contenidos, en ocasiones sin previo aviso, si tiene indicios de una supuesta ilegalidad, o si lo considera pertinente.

En resumen, de acuerdo con la LSSI, tras requerimiento por la autoridad competente, el proveedor de servicios de computación en la nube tiene el deber de colaborar con las autoridades públicas para bloquear el acceso a los contenidos ilícitos y/o retirarlos de la Red o de su acceso por otros usuarios, (art. 11 LSSI), derivándose responsabilidades para los que no actuaran con diligencia para imposibilitar el acceso a estos contenidos (art. 16 LSSI)[55].

En cambio, si por razón de la prestación del servicio, el proveedor ha comprobado la existencia ciertos contenidos depositados en su sistema por un usuario final que pueden infringir la legislación vigente o lesionar derechos de terceros, no tiene la obligación legal de decidir sobre la difusión o retirada de los contenidos alojados por su cliente. No obstante, si estos contenidos no solo son susceptibles de infringir la legislación, sino que son manifiestamente ilegales (pornografía infantil, preparación de actos de terrorismo, etc.), y cuando pueda probarse que tuvo conocimiento de estas actividades y no lo denunció, podría alegarse que ha tenido conocimiento efectivo de acuerdo con el art. 16.1 LSSI. Además, podría ser responsable, en atención al carácter general del art. 13.1 de la LSSI y al resto del ordenamiento jurídico, a efectos civiles (arts. 1101, 1902 y siguientes del Código Civil) y penales (art. 262 LECr)[56].

---

55 Para BUSTO LAGO, la exclusión de responsabilidad dependerá de que el prestador de servicios de intermediación no sea autor del contenido ilícito ni el contenido se elabore por cuenta suya, de su colaboración y cooperación con las autoridades, y de su reacción diligente al interrumpir el acceso al contenido ilícito. BUSTO LAGO, J.M., "La responsabilidad civil de los prestadores de servicios de la sociedad de la información (ISPs), *Tratado de Responsabilidad Civil,* Tomo II, (Coord. Reglero Campos), Navarra, 2008, págs. 1003 a 1012. Según CONDE y DÍEZ, existirá responsabilidad para el prestador de servicios de intermediación cuando tenga conocimiento efectivo de la ilicitud de los contenidos o datos almacenados, o cuando constituyan una lesión a terceros susceptible de indemnización. CONDE BUESO, I; DÍEZ LÓPEZ, I, "Artículo 16: la responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos", *La nueva Ley de Internet. Comentarios a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico*, (Coord. CREMADES J, González Montes, J), Madrid, 2003, pág. 285.

56 Art. 13.1 LSSI. "Los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley".

El proveedor de servicios *cloud* tampoco tiene la obligación de supervisión de datos ni la realización de búsquedas activas o indagación en datos migrados por los clientes. Además, quedará a su discrecionalidad la suspensión del servicio o la retirada de contenidos ilícitos del usuario, y la instauración de mecanismos que permitan a otros usuarios avisar al proveedor de la existencia de contenidos lesivos.

Por nuestra parte, consideramos recomendable para el proveedor la adopción de mecanismos que permitan a otros usuarios informar al proveedor sobre la difusión, a través del servicio *cloud*, de eventuales contenidos ilícitos, y que se lleve a cabo la efectiva investigación interna de tales avisos remitidos por otros usuarios, a modo de buenas prácticas, y como demostración de su deber de diligencia profesional ante eventuales reclamaciones de responsabilidad.

4.- DATOS DIGITALES EN LA NUBE, PROPIEDAD INTELECTUAL Y SECRETO COMERCIAL: PROTECCIÓN DE LOS DATOS Y RESTRICCIONES AL USO Y A LA EXPLOTACIÓN DE LOS CONTENIDOS EN EL CONTRATO DE SERVICIOS *CLOUD*

Debido a las muchas posibilidades que ofrece la computación en la nube para crear, almacenar y compartir contenidos, aparecen dudas sobre quién es el titular de unos datos u otros, y qué usos se permiten de estos datos y a quién. Tanto usuario como proveedor creen tener razones para pensar que ostentan todo o cierto grado de control en cuanto a los datos creados o migrados por el primero; o alojados o puestos a disposición en los sistemas del segundo.

Las cláusulas de los contratos no siempre ayudan a disipar todas las incertidumbres sobre esta materia, puesto que su redacción a menudo funciona como simple recordatorio de la normativa existente sobre propiedad intelectual (y en casos en los que entran en juego diferentes jurisdicciones, incluso contradiciéndola). Esta parte del trabajo se centrará en la problemática derivada de las condiciones de uso, titularidad y control de las diferentes categorías de contenidos creadas, migradas o puestas a disposición (tanto por el proveedor como por el usuario) en la nube[57].

57 En este trabajo se tratarán conceptos de propiedad intelectual, así como otros conceptos (propiedad industrial, secreto empresarial, etc.), de manera transversal e instrumental, para aplicarlos a los servicios de computación en la nube.

4.1.- Generalidades sobre la propiedad intelectual e industrial

La Organización Mundial de la Propiedad Intelectual (OMPI) define la propiedad intelectual como "los derechos legales que resultan de procesos intelectuales en los campos industrial, científico, literario y artístico"[58].

A menudo se toman como equivalentes los términos "derechos de autor" y *copyright*. Aunque, a grandes trazos, las prerrogativas que otorgan a los titulares originarios son prácticamente equivalentes en los sistemas continental y anglosajón respectivamente (sin perjuicio de las particularidades de cada una de las legislaciones nacionales), existen matices que los diferencian[59]. En concreto, nos referimos a la concepción que tiene el *Common Law* sobre la obra artística, industrial o científica, entendida como un bien de consumo. Así, el *copyright* afecta solo a los derechos puramente económicos, y, como tal, permite su íntegra transmisión, así como la atribución de la titularidad en origen a personas jurídicas. En cambio, los derechos morales que forman parte del derecho de autor evitan la total desvinculación entre el autor y su obra, siendo el mayor exponente de esta afirmación el derecho de paternidad[60]. Esta diferenciación debe tenerse en cuenta en nuestro trabajo, dada la

58 WIPO *Intellectual Property Handbook* [en línea]. Disponible en: <http://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf> [Fecha de consulta: 27 de abril de 2017].

59 La doctrina ha distinguido entre derecho de autor y *copyright*: "El derecho de autor, tal como lo conocemos hoy en día, se diferencia del modelo de copyright, y está caracterizado esencialmente por los siguientes fundamentos: 1. El derecho de autor corresponde a una concepción jurídica de la teoría filosófica individualista, de derecho natural, en donde el derecho surge por la labor intelectual; en esa medida, la protección es automática al momento de la creación, y no se requieren formalidades para la existencia del derecho; 2. El derecho de autor está compuesto por derechos patrimoniales, y especialmente por derechos morales de autor relacionados con su esfera personal y que protegen su individualidad, su honor y prestigio; 3. La protección que se otorga está limitada en el tiempo, y tiene como base la vida del autor y mínimo cincuenta años *post mortem auctoris*. (...) Debe precisarse que existen dos figuras jurídicas similares a nivel internacional, pero no idénticas, y que permiten circunscribir mejor el objeto de estudio. El *copyright* y el derecho de autor obedecen a un propósito jurídico similar, pero pertenecen a sistemas legales diferentes: el primero al derecho anglosajón o *common law*, y la segunda figura a la tradición del derecho continental europeo". PABÓN CADAVID, J. Antonio, "Aproximación a la historia del derecho de autor. Antecedentes normativos", *Revista de la propiedad inmaterial*, núm. 13, Colombia, 2009, págs. 69 a 104. Para un estudio más detallado, nos remitimos a WAELDE, Charlotte; LAURIE, Graeme (et al.), *Contemporary Intellectual Property Law and Policy*, 3ª edición, Reino Unido, 2014, 1104 págs. STONE, Peter; *Copyright Law in the UK and European Community*, 1ª edición, Holanda, 1990, 293 págs.

60 En la legislación nacional, el derecho de paternidad aparece regulado en el art. 14.2 del TRLPI. "Corresponden al autor los siguientes derechos irrenunciables e inalienables: (…) 2.- Determinar si tal

tan frecuente multinacionalidad de los diferentes actores involucrados en la relación contractual de servicios de computación en la nube[61].

---

divulgación [de su obra] ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente". En el ámbito del Derecho Internacional, aparece recogido en el art. 6 bis del Convenio de Berna de 1971, junto a los demás derechos morales del autor: "1.- Independientemente de los derechos patrimoniales del autor, e incluso después de la cesión de estos derechos, el autor conservará el derecho de reivindicar la paternidad de la obra y de oponerse a cualquier deformación, mutilación u otra modificación de la misma o a cualquier atentado a la misma que cause perjuicio a su honor o a su reputación. 2.- Los derechos reconocidos al autor en virtud del párrafo 1 serán mantenidos después de su muerte, por lo menos hasta la extinción de sus derechos patrimoniales, y ejercidos por las personas o instituciones a las que la legislación nacional del país en que se reclame la protección reconozca derechos. Sin embargo, los países cuya legislación en vigor en el momento de la ratificación de la presente Acta o de la adhesión a la misma, no contenga disposiciones relativas a la protección después de la muerte del autor de todos los derechos reconocidos en virtud del párrafo 1 anterior, tienen la facultad de establecer que alguno o algunos de esos derechos no serán mantenidos después de la muerte del autor". Como esta redacción deja entrever, no todos los países, en especial algunos pertenecientes al sistema anglosajón, reconocen la existencia de derechos morales, tal y como pone de manifiesto la excepción del art. 9.1 del Acuerdo de la Organización Mundial del Comercio sobre los Aspectos de Derechos de Propiedad Intelectual relacionados con el comercio: "Los Miembros observarán los artículos 1 a 21 del Convenio de Berna (1971) y el Apéndice del mismo. No obstante, en virtud del presente Acuerdo ningún Miembro tendrá derechos ni obligaciones respecto de los derechos conferidos por el artículo 6 bis de dicho Convenio ni respecto de los derechos que se derivan del mismo (...)".

61 Llegados a este punto, consideramos apropiado realizar un apunte terminológico. La protección de los datos informáticos, como es sabido, recae sobre un objeto incorpóreo: la creación intelectual, desde el mismo momento en que esté realizada y sea perceptible (ya sea de forma visual o tras requerir un procedimiento técnico que permita su expresión fuera de la mente del autor). Por ello, y aunque se hayan extendido en el sector *cloud* las expresiones "propiedad de los contenidos" o "propiedad de los datos", sobre todo en los términos contractuales que delimitan las responsabilidades entre cliente y proveedor a efectos de proteger la información del cliente o de retornarla una vez finalizado el contrato. es necesario realizar ciertas precisiones respecto del uso del término "propiedad". Como deja patente el artículo 3 de la TRLPI ("Los derechos de autor son independientes, compatibles y acumulables con:1.- La propiedad y otros derechos que tengan por objeto la cosa material a la que está incorporada la creación intelectual"), la propiedad intelectual pertenece a una categoría especial de propiedad, cuya característica esencial es la inmaterialidad de la obra objeto de derechos, pero la propiedad en sí misma es predicable únicamente de cosas corpóreas. La misma idea se extrae tanto del art. 334 del Código Civil ("La propiedad es el derecho de gozar y disponer de una cosa, sin más limitaciones que las establecidas en las leyes". El mismo Código, en su art. 333, establece que "Todas las cosas que son o pueden ser objeto de apropiación se consideran como bienes muebles o inmuebles"), como de la definición formulada por la Real Academia Española de la Lengua. Resumiendo, no estaríamos hablando concretamente de "propiedad de los datos o de la información", sino de "titularidad de los datos o de la información". Por otra parte, son frecuentes los términos de servicio en los que los proveedores, con el propósito de facilitar la comprensión al usuario (sobre todo consumidor), hablan de "tus datos", "tus contenidos". Por ejemplo, los términos de servicio del software como servicio de almacenamiento Dropbox para particulares utilizan la expresión "tus cosas" para referirse a archivos y contenidos digitales del usuario: "Nuestros Servicios están diseñados para que te resulte sencillo almacenar Tus cosas, colaborar con otras personas y trabajar con varios dispositivos. Para que eso sea posible, almacenamos, procesamos y transmitimos Tus cosas (por

4.1.1.- Las obras protegidas por el derecho de autor

Las obras protegidas por el derecho de autor están enumeradas en el art. 10 del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (en adelante, TRLPI), aunque la propia Ley reconoce que es una lista abierta[62]. Cualquier obra susceptible de digitalizarse puede crearse, formar parte o estar alojada en sistemas de computación en la nube: textos, composiciones musicales, dibujos, proyectos y diseños, planos, obras fotográficas (y meras fotografías), obras audiovisuales, etc.[63] La ley considera los programas de ordenador como obra, aunque exige ciertos requisitos para que se conviertan en objeto de protección. También las bases de datos son objeto de una regulación especial en cuanto a obras susceptibles de generar derechos de propiedad intelectual. Por su importancia en las relaciones entre las partes, trataremos con

ejemplo, archivos, mensajes, comentarios y fotos), así como cualquier información relacionada". Del mismo modo, los términos de la red social Facebook informan que "eres el propietario de todo el contenido y la información que publicas en Facebook, y puedes controlar cómo se comparte a través de la configuración de la privacidad y de las aplicaciones". Disponibles respectivamente en: <https://www.dropbox.com/es_ES/privacy> y <https://www.facebook.com/legal/terms/update>. [Fecha de consulta: 27 de abril de 2017].

62 Art. 10 del TRLPI. "Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas: a) Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, explicaciones de cátedra y cualesquiera otras obras de la misma naturaleza. b) Las composiciones musicales, con o sin letra. c) Las obras dramáticas y dramático-musicales, las coreografías, las pantomimas y, en general, las obras teatrales. d) Las obras cinematográficas y cualesquiera otras obras audiovisuales. e) Las esculturas y las obras de pintura, dibujo, grabado, litografía y las historietas gráficas, tebeos o cómics, así como sus ensayos o bocetos y las demás obras plásticas, sean o no aplicadas. f) Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería. g) Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia. h) Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía. i) Los programas de ordenador".

63 Por otra parte, la protección en España no exige, por tanto, que la obra (que puede ser un contenido digital) esté incorporada en un soporte material, aunque si es así, este soporte será objeto del derecho tradicional de propiedad, acumulable a los derechos de autor (art. 56 TRLPI Art. 3.1 del TRLPI*:* "Los derechos de autor son independientes, compatibles y acumulables con: 1.) La propiedad y otros derechos que tengan por objeto la cosa material a la que está incorporada la creación intelectual (...)". En países donde rige el sistema anglosajón, como Inglaterra o EEUU, se exige que la obra esté grabada. Copyright, Designs and Patents Act, 1988, s. 3 (2): "Copyright does not subsist in a literary, dramatic or musical work unless and until it is recorded, in writing or otherwise; and references in this Part to the time at which such a work is made are to the time at which it is so recorded". Mejor explicado aparece en la US Copyright Law, § 102: "Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device". COLSTON, Catherine; MIDDLETON; Kirsty; *Modern Intellectual Propierty Law,* 2ª edición, Londres, 2005, 808 págs. Llibre UCLondon. 253*

detalle en un apartado posterior tanto las bases de datos como los programas de ordenador atendiendo a las consecuencias jurídicas de su aportación en el sistema *cloud* por el usuario o por el proveedor, y a su reflejo contractual.

La exigencia de originalidad del art. 10.1, requisito *sine qua non* de la consideración de una obra como objeto de estos derechos (sin perjuicio de la protección otorgada por el art. 11 a las obras derivadas), hace necesario diferenciarla de otros contenidos sin originalidad subjetiva: ideas, procedimientos, conceptos matemáticos, lenguajes informáticos, funcionalidades, algoritmos, listados telefónicos, estadísticas objetivas, listados de productos, cifras financieras...

4.1.2.- La protección de los secretos de empresa

La protección de estos activos tan importantes (origen de futuras invenciones patentables, marcas registradas, diseños, etc.) es esencial para la protección de las empresas tecnológicas contra el espionaje industrial, pero esta información a menudo encuentra trabas para ampararse bajo el marco de la propiedad intelectual e industrial.

La normativa sobre competencia desleal (que citaremos más adelante) y la normativa penal[64] acotan ciertas actividades prohibidas, pero tampoco son la panacea para muchos problemas jurídicos derivados de la computación en la nube relativos a los secretos de empresa[65].

La Unión Europea, consciente de la importancia de proteger la información reservada de alto valor comercial, y de la falta de armonización, ha aprobado la Directiva 2016/943 de 8 de junio de 2016 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas[66]. Esta Directiva

64 En especial, los artículos 270 a 277 de la Ley orgánica 10/1995, de 23 de noviembre, del Capítulo XI del título del Código Penal: "De los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores.

65 Por ejemplo, qué sucede cuando un tercero de buena fe adquiere una información cuyo origen inicial es ilícito; qué sucede con esa información si aun no se ha sometido a conocimiento público, una vez terminado el contrato con el proveedor: si esa información debe devolverse o debe destruirse; qué responsabilidades pueden derivarse si esa información pasa a ser de conocimiento público a causa de una actividad ilegítima; cómo se calculan las cantidades indemnizatorias, etc.

66 La propia Comisión aclara que los secretos de empresa no están sujetos al derecho de propiedad

pretende armonizar los medios civiles a través de los cuales las víctimas de apropiaciones indebidas de secretos comerciales puedan protegerse, y que permitan detener los usos ilegítimos y potenciales divulgaciones de los secretos, la retirada del mercado de bienes fabricados gracias a la obtención ilegal de secretos comerciales, y el derecho a obtener una compensación por los daños causados.

En la Directiva se definen los secretos comerciales como "la información que reúna todos los requisitos siguientes: a) ser secreta en el sentido de no ser, en su conjunto o en la configuración y reunión precisas de sus componentes, generalmente conocida por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información en cuestión, ni fácilmente accesible para estas; b) tener un valor comercial por su carácter secreto; c) haber sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control" (art. 2)[67].

Esta Directiva está alineada con el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), cuya definición de secreto comercial, en su art. 39.2[68], ha servido de referencia en muchas ocasiones a los tribunales españoles[69]. De acuerdo con este Tratado, suscrito por los

---

intelectual, y no gozan de protección desde el mismo momento de la creación. Más información en la página web oficial de la Comisión Europea y en la solución a las FAQs sobre secreto empresarial [en línea]. Disponible en: <http://ec.europa.eu/growth/industry/intellectual-property/trade-secrets/>. [Fecha de consulta: 27 de abril de 2017].

67 Algunos ejemplos de información que puede considerarse secreto empresarial o comercial pueden ser: resultados de estudios de marketing, objetivos financieros, listas de productos y sus precios o fechas de lanzamiento, compuestos químicos, recetas y fórmulas, procesos internos de manufactura, alianzas del negocio, etc.

68 Art. 39.2 del ADPIC. "Las personas físicas y jurídicas tendrán la posibilidad de impedir que la información que esté legítimamente bajo su control se divulgue a terceros o sea adquirida o utilizada por terceros sin su consentimiento de manera contraria a los usos comerciales honestos, en la medida en que dicha información: a) sea secreta en el sentido de que no sea, como cuerpo o en la configuración y reunión precisas de sus componentes, generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; y b) tenga un valor comercial por ser secreta; y c) haya sido objeto de medidas razonables, en las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la controla".

69 La sentencia de la Audiencia provincial de Madrid 231/2010 de 15 de octubre reconoce la inexistencia de un concepto legal de secreto empresarial, así como la falta de cobertura de ciertos actos como desleales. En la demanda se narraban una serie de hechos que la actora consideraba actos desleales por violación de secretos y por inducción a la infracción contractual, que se alegaba que habrían situado a la demandante en una posición de desventaja competitiva y pérdida de ingresos. Las pretensiones de la demandante no prosperaron en la primera instancia ya que, en esencia, en la resolución recurrida no consideró acreditado que hubiesen mediado conductas desleales imputables a los demandados. En su motivo Sexto, la Audiencia define lo que entiende como secreto empresarial "Ante la falta de definición legal de secretos industriales o empresariales podemos entender como tales el conjunto de informaciones o conocimientos que no son de dominio público

Estados miembros de la Organización Mundial del Comercio, las personas físicas y jurídicas pueden proteger sus secretos con valor comercial ante revelaciones, obtenciones o usos ilegítimos y contrarios a las prácticas comerciales honestas.

Actualmente, el secreto empresarial está protegido en aquellos casos en que alguien ha obtenido la información a través de medios ilegales (infracción del deber de confidencialidad[70] o de exclusividad de empleados, socios o administradores[71]; soborno, espionaje, robo, etc.), como acto de competencia desleal[72] o cuando la

---

y que son necesarios para la fabricación o comercialización de un producto, para la producción o prestación de un servicio o bien para la organización y financiación de una empresa". A continuación, enumera los requisitos exigidos por el ADPIC para considerar la información como secreto comercial: "Siguiendo el artículo 39.2 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC; BOE de 24 de enero de 1995), para que la información empresarial pueda considerarse secreto y sea susceptible de protección es necesario que concurran los siguientes requisitos: 1) que no sea generalmente conocida ni fácilmente accesible para personas introducidas en los círculos en que normalmente se utiliza el tipo de información en cuestión; 2) que tenga un valor comercial por ser secreta; y 3) que haya sido objeto de medidas razonables, atendidas las circunstancias, para mantenerla secreta, tomadas por la persona que legítimamente la controla (también, en sentido análogo, artículo 1.7 del Reglamento CEE núm. 556/89, de la Comisión, de 30 de noviembre de 1988, relativo a la aplicación del apartado 85 del Tratado a determinadas categorías de acuerdos de licencia de *know-how)"*. En cuanto a la clasificación de los actos como desleales en aplicación del art. 13 de la LCD, dice la sentencia que "ni las informaciones que formen parte de las habilidades, capacidades y experiencia profesionales de carácter general de un sujeto, ni el conocimiento y relaciones que pueda tener con la clientela, aunque lo haya adquirido en el desempeño de sus funciones para otro, pueden ser consideradas como secreto empresarial". La demanda de apelación se desestimó por falta de acreditación del valor comercial de la información y de su sometimiento a medidas especiales que garantizasen su secreto.

70 Se encuentra en el art. 5 del Estatuto de los trabajadores, como materialización de sus deberes de buena fe y diligencia. Ver subapartado "La confidencialidad de los datos del cliente y las solicitudes de acceso de terceros", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

71 Se regula en el art. 232 del Real Decreto-Legislativo 1/2010 de Sociedades de Capital: "Los administradores, aun después de cesar en sus funciones, deberán guardar secreto de las informaciones de carácter confidencial, estando obligados a guardar reserva de las informaciones, datos, informes o antecedentes que conozcan como consecuencia del ejercicio del cargo, sin que las mismas puedan ser comunicadas a terceros o ser objeto de divulgación cuando pudiera tener consecuencias perjudiciales para el interés social".

72 Artículos 13 y 14 de la Ley 3/1991 de Competencia Desleal. "Art. 13.-Violación de secretos. 1. Se considera desleal la divulgación o explotación, sin autorización de su titular, de secretos industriales o de cualquier otra especie de secretos empresariales a los que se haya tenido acceso legítimamente, pero con deber de reserva, o ilegítimamente, a consecuencia de alguna de las conductas previstas en el apartado siguiente o en el artículo 14. 2. Tendrá asimismo la consideración de desleal la adquisición de secretos por medio de espionaje o procedimiento análogo. 3. La persecución de las violaciones de secretos contempladas en los apartados anteriores no precisa de la concurrencia de los requisitos establecidos en el artículo 2. No obstante, será preciso que la violación haya sido efectuada con ánimo de obtener provecho, propio o de un tercero, o de perjudicar al titular del secreto. Artículo 14. Inducción a la infracción contractual. 1. Se considera desleal la inducción a trabajadores, proveedores, clientes y demás obligados, a infringir los deberes

creación es susceptible de ser registrada, patentada o protegida por la propiedad industrial; o si por fin adquiere el matiz de "obra" y puede resultar enmarcable como tal en la legislación de propiedad intelectual; o por su contenido puede considerarse protegido por otra normativa sectorial (banca, seguros, datos personales, etc.). Quedan fuera del secreto de empresa la información no relevante[73], así como los conocimientos adquiridos a través de la capacitación y formación de los trabajadores, y los conocimientos accesibles a través de un sector profesional en particular[74].

---

contractuales básicos que han contraído con los competidores. 2. La inducción a la terminación regular de un contrato o el aprovechamiento en beneficio propio o de un tercero de una infracción contractual ajena sólo se reputará desleal cuando, siendo conocida, tenga por objeto la difusión o explotación de un secreto industrial o empresarial o vaya acompañada de circunstancias tales como el engaño, la intención de eliminar a un competidor del mercado u otras análogas".

73 Según el Tribunal Supremo, en su sentencia 97/2009, de 25 de febrero, en la que los demandados, antiguos trabajadores de la empresa de ascensores Giesa-Schlinder, constituyen una sociedad que prospera, presuntamente, gracias al uso de listados de clientes y precios de la primera. Muchos clientes resolvían los contratos de aquella para trabajar con la nueva empresa de los exempleados. "Se imputa violación de secretos que calificarían la conducta como desleal y que en el caso se habría de traducir en la explotación de los listados de clientes y de otras informaciones sobre precios y condiciones, que habrían de tener la consideración de secretos empresariales a los efectos de poder ser encuadrada su explotación en las previsiones del precepto señalado. (...) Ha de destacarse que los demandados han podido tener acceso legítimo, con lo que se trasladaría la cuestión al punto de determinar si pesaba sobre los demandados un especial deber de reserva que, en el contexto en que se produce, no parece haya de extenderse a los conocimientos y relaciones que hayan adquirido precisamente en el desempeño de las funciones, además de que no se trata, en puridad, de secretos empresariales, pues la información utilizada no es realmente secreta, en términos de utilidad y valor que el sujeto en cuestión [la actora] ha conferido a la información en cuestión, desde el punto y hora en que no ha tomado medidas para salvaguardarla o protegerla". Se desestima la pretensión de la demandante de declarar la actividad como desleal de acuerdo con el art. 13 LCD "por no resultar probado, ni haber aportado la actora datos para ello, que la actividad realizada por la demandada con posterioridad a la finalización del contrato constituía la explotación del *know-how* de la actora o de otros secretos industriales o empresariales".

74 La sentencia de la Audiencia Provincial de Barcelona núm. 443/2005, de 26 de octubre, en un caso en el cual la empresa "*Pronovias"* denuncia una copia de modelos originales introducidos en el mercado por parte de antiguos trabajadores. "Hay que anotar también, como hemos indicado en otras resoluciones, que deben distinguirse del secreto empresarial aquellas informaciones que formen parte de las habilidades, capacidades y experiencia profesionales de carácter general de un sujeto. En este sentido, las habilidades, capacidades, experiencia y conocimiento del sector o actividad que componen la formación y capacitación profesional del trabajador (que sin duda por esas razones es incorporado a la empresa de la competencia), son de libre e incluso necesario uso por el mismo, con el consiguiente aprovechamiento por la nueva empresa que lo emplea, en el ulterior desarrollo de su vida laboral, normalmente dedicada al mismo sector en el que ha adquirido aquellos valores. (...) Esas capacidades o habilidades son independientes, por ello, de los secretos empresariales, que deben distinguirse de aquellos conocimientos adquiridos por el trabajador y, por tanto, necesarios para hacer uso de su derecho constitucional a desarrollar un trabajo, aunque sea en una empresa de la competencia. (...) La dificultad reside, naturalmente, en deslindar, de un lado, los conocimientos que objetivamente pertenecen a la empresa y que están protegidos como secretos empresariales y, de otro, el conjunto de conocimientos y capacidades personales del trabajador, cuya

En la nube, son muchos los actores que tienen acceso a copias o a archivos electrónicos que comprenden secretos comerciales, con lo cual el riesgo de filtraciones puede llegar ser considerable. Sin embargo, en ninguno de los contratos examinados en el curso de este trabajo aparecen cláusulas específicas para este tipo de información reservada. Así, la protección contractual del secreto empresarial se encuentra diluida entre las referencias a la propiedad intelectual (de cuya protección, como hemos observado, quedará excluida en muchos casos) y el deber de confidencialidad.

Por otro lado, cuestiones como la ingeniería inversa[75], tan habitual entre empresas del sector tecnológico y a menudo prohibidas en las políticas de uso adecuado de los contratos *cloud*, se encuentran en un limbo normativo. Con la nueva Directiva 2016/943, antes mencionada, sería legal su realización, aunque podría limitarse por vía contractual[76]. Esta nueva regulación también puede contribuir a reforzar la posición de muchos pequeños empresarios que no poseen capacidad de negociación a la hora de contratar servicios en la nube, para que se mantenga la confidencialidad de su información dentro de nubes públicas[77].

4.1.3.- La propiedad industrial

La propiedad industrial regula diferentes elementos relacionados con la actividad empresarial: las marcas y nombres comerciales, las invenciones (patentes,

---

utilización precisa en el ejercicio de su derecho al trabajo".

75 Como hemos mencionado en apartados anteriores, la ingeniería inversa consiste en la obtención de información sobre los componentes de fabricación y el mecanismo de funcionamiento de un producto físico o de un programa informático a través de un examen directo del producto o del dispositivo que contiene el programa cuando se obtiene o se usa de forma legal. (Definición propia).

76 En el Considerando 16, la Directiva afirma: "En interés de la innovación y a fin de promover la competencia, lo dispuesto en la presente Directiva no debe generar ningún derecho de exclusividad sobre los conocimientos técnicos o la información protegidos como secretos comerciales. Así pues, sigue siendo posible el descubrimiento independiente de la misma información o de los mismos conocimientos técnicos. La ingeniería inversa de un producto obtenido lícitamente debe considerarse un medio lícito de obtener información, excepto cuando se haya convenido de otro modo por contrato. No obstante, la libertad de adoptar este tipo de cláusulas contractuales puede limitarse por ley".

77 Ello es así gracias a la sanción de ciertos comportamientos relacionados con el acceso u obtención no autorizada de información calificada como secreto profesional y a la utilización y revelación de esta información (arts. 2, 4.4 y 4.5 de la Directiva 206/943). La Directiva también establece las medidas provisionales y cautelares, los procedimientos y los recursos a disposición del titular del secreto comercial (arts. 6 a 15).

modelos de utilidad, etc.) y los diseños industriales (dibujos y modelos industriales)[78]. Algunas obras susceptibles de registrarse como propiedad industrial ya están protegidas previamente por derechos de autor (art. 3.2 y 10 TRLPI), pero la propiedad industrial dota a estas obras de una protección extraordinaria, otorgándole ciertas prerrogativas sobre sus competidores en el mercado en relación a la marca, invención o diseño patentados.

La regulación española de estos elementos se encuentra en la Ley 11/86 de 20 de marzo, de patentes de invención y modelos de utilidad (para patentes y modelos), la Ley 17/2001 de 7 de diciembre de marcas (para signos distintivos), y la Ley 20/2003, de 7 de julio, de protección jurídica del diseño industrial (para diseños de productos). El Acuerdo de los Derechos de la Propiedad Intelectual relacionados con el Comercio (ADPIC) también regula ciertos aspectos relacionados con las marcas, invenciones y patentes.

4.1.4.- Las licencias de uso

Tanto los titulares de derechos de propiedad industrial como los de derechos de autor pueden licenciar o ceder sus derechos de propiedad y explotación[79]. La OMPI define un acuerdo de licencia como "una asociación entre un titular de derechos de propiedad intelectual (licenciante) y otra persona que recibe la autorización de utilizar dichos derechos (licenciatario) a cambio de un pago convenido de antemano (tasa o regalía)"[80], y lo considera un elemento vital de la estrategia comercial de una PYME. Existen

78 Las marcas y nombres comerciales protegen combinaciones gráficas y/o denominativas que ayudan a distinguir en el mercado unos productos o servicios de otros similares ofertados por otros agentes económicos. Las patentes y modelos de utilidad protegen invenciones consistentes en productos y procedimientos susceptibles de reproducción y reiteración con fines industriales. Los diseños industriales protegen la apariencia externa de los productos. (Definiciones facilitadas por el sitio web oficial de la Oficina Española de Patentes y Marcas). <http://www.oepm.es/es/propiedad_industrial/propiedad_industrial/index.html>. [Fecha de consulta: 27 de abril de 2017].

79 La estancada Propuesta de Código Mercantil introduce el concepto de licencia de bienes inmateriales, en su art. 536.1: "Por el contrato de licencia, el titular de un derecho sobre un bien inmaterial, denominado licenciante, autoriza a un tercero, denominado licenciatario, para utilizarlo o explotarlo durante un tiempo determinado a cambio de un precio, manteniendo el licenciante la titularidad del derecho".

80 Fuente: sitio web oficial de la OMPI. Disponible en: <http://www.wipo.int/sme/es/ip_business/licensing/licensing.htm> [Fecha de consulta: 27 de abril de 2017].

distintos tipos de licencias, en atención a su objeto: tecnológicas (para invenciones y diseños industriales), sobre marcas y sobre derechos de autor. El licenciante de derechos retiene su titularidad, pero autoriza ciertos usos durante un tiempo y en la forma fijada contractualmente[81].

En el ámbito de los contratos de computación en la nube, son frecuentes las cláusulas que conforman verdaderas licencias de uso, cuya duración se presume durante el tiempo de subsistencia de la relación jurídica entre las partes. En nuestro examen de contratos hemos identificado algunas licencias considerablemente amplias, pero no hemos detectado ninguna cesión de titularidad de derechos[82]. Más adelante trataremos la cuestión de las licencias en mayor profundidad, en relación con los usos y titularidad de los datos aportados por el usuario y por el proveedor de los servicios en la nube.

4.2.- Contenidos generados fuera de la nube y migrados por el usuario[83]

En la utilización de sistemas de computación en la nube es necesario el flujo de información entre el usuario y el entorno *cloud* del proveedor para procesar, almacenar y compartir los datos. De acuerdo con lo expuesto en el apartado anterior, la información que el usuario introduce en el sistema es susceptible de ser objeto de derechos de propiedad intelectual que probablemente hayan nacido en un momento anterior a su ingreso en la nube. A continuación observaremos distintas consecuencias jurídicas que pueden derivarse de la utilización en la nube de obras

81 En relación a la distinción entre el contrato de computación en la nube y el contrato de licencia de uso de software, nos remitimos al capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

82 A continuación, un ejemplo de licencia de uso de contenidos del usuario, localizado en las condiciones de uso de la red social Instagram [en línea]. "Instagram no reclama la propiedad de ningún contenido que publiques en el servicio o a través de este. En su lugar, por la presente otorgas a Instagram una licencia totalmente pagada, sin derechos de autor, no exclusiva, transferible, con posibilidad de ser subotorgada y aplicable globalmente para utilizar el contenido que publiques en el servicio o a través de este, conforme a la política de privacidad del servicio disponible en (...)". Condiciones de uso de la red social Instagram [en línea]. Disponible en: <https://help.instagram.com/478745558852511>. [Fecha de consulta: 2 de mayo de 2017].

83 Con el término usuario nos referimos a aquellas personas físicas que realicen un uso material del servicio de computación en la nube, pudiendo ser ellos mismos los suscriptores de los servicios *cloud*, o utilizándolos con autorización del pequeño empresario suscriptor, como sería el caso de los empleados de este.

objeto de derechos de autor, dependiendo de quién sea su titular.

4.2.1.-Los contenidos creados por el usuario y migrados a la nube. Las licencias de uso de contenidos del usuario de la nube

Si se trata de contenidos propios, el usuario autor puede disponer de su obra, y comunicarla o explotarla (dentro o fuera de la nube) como mejor le parezca y con quien desee, determinando las condiciones en las cuales autoriza el uso de esa obra a través de una licencia. El incumplimiento de estas condiciones supondrá una infracción de derechos de propiedad intelectual y una infracción contractual[84].

A falta de estas condiciones (es decir, si el autor no establece ningún tipo de licencia u otras condiciones de utilización de su obra), no se otorga ninguna autorización para usar esa obra y el autor, como tal, conserva la plena disposición de todos los derechos. Sin embargo, podría también entenderse que el autor está autorizando implícitamente que esa obra pueda ser utilizada y explotada según los usos del sector, con lo cual, en el contexto de redes sociales, coincidimos con otros autores en que puede significar que la obra sea objeto de descargas y acceso en línea por parte de los usuarios, objeto de enlaces a la página web[85]. La dificultad, en este contexto, radica en el seguimiento de los usos realizados en cadena y en la identificación de los posibles infractores. Igualmente, la obra podrá utilizarse sin necesidad de autorización del autor en los casos permitidos por el Texto Refundido de la Ley de Propiedad Intelectual (arts. 31 a 40 TRLPI), teniendo que respetarse los derechos morales, que son irrenunciables e inalienables[86].

Como se ha dicho, el usuario que ha creado contenidos fuera de la nube y

84 Ver apartado "Las licencias de uso", en este mismo capítulo.

85 Los usos de contenidos ajenos "recibidos" a través del servicio *cloud* pueden implicar un acceso lícito a la obra y la copia privada permitida por el art. 31.2 del TRLPI (descargarla en el disco duro del dispositivo o imprimirla para uso no colectivo ni lucrativo, etc.). Al compartirse obras ajenas se realiza un uso que va más allá del mero acceso y la descarga. Así, esta obra no podría ponerse accesible a terceros en un programa tipo *peer to peer*, puesto que supone un nuevo acto de comunicación pública; ni colgar esa obra en un sitio web distinto, puesto que supone un nuevo acto de reproducción y puesta a disposición del público. Sí se podrá, en cambio, adjuntar esa obra en un correo electrónico para compartirla, por ejemplo, con un amigo, o introducir en el sitio web un enlace que dirija al sitio web con la obra de origen. XALABARDER PLANTADA, Raquel; "Redes sociales y Propiedad Intelectual", *Derecho y redes sociales,* (Coord. Artemi Rallo, Ricard Martínez), 1ª edición, Navarra, 2010, pág. 344.

86 XALABARDER PLANTADA, Raquel; *Redes sociales..., op. cit.*, pág. 344.

posteriormente los ha migrado o almacenado a los sistemas del proveedor *cloud* no pierde, en principio, sus derechos de autor sobre esos contenidos. Las cesiones de titularidad a través de contratos de computación en la nube y de redes sociales no son habituales. Sin embargo, sí lo son las licencias de uso en favor del proveedor o de terceros incluidas como cláusulas generales en el contrato, algunas de ellas no demasiado transparentes en su redacción, en las que, como veremos más adelante, el proveedor se reserva derechos de uso y/o explotación sobre contenidos migrados por el usuario y de los cuales este es titular (como pueden ser fotografías, vídeos, textos y demás obras creadas por él).

Todo acuerdo de licencia contendrá una previsión del uso de los contenidos que el cliente pone a disposición del proveedor. Las facultades que el usuario concede suelen consistir en el acceso para tareas técnicas o verificación de PUA, almacenamiento, copias de seguridad, replicado en diferentes servidores, transferencia entre sistemas, compartición de contenidos entre usuarios (como parte de las funcionalidades del servicio), etc.

Sin embargo, estas licencias resultan particulares porque no las redacta el licenciante, sino el licenciatario. Así, en algunos casos el proveedor se reserva el derecho de crear obras derivadas o el derecho a la comunicación pública y distribución de contenidos[87]. Aunque suelen ceñirse a la prestación del servicio[88], en

87 Condiciones generales comunes para todos los productos y servicios Google [en línea]: "Al subir, almacenar o recibir contenido o al enviarlo a nuestros servicios o a través de ellos, concedes a Google (y a sus colaboradores) una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas (por ejemplo, las que resulten de la traducción, la adaptación u otros cambios que realicemos para que tu contenido se adapte mejor a nuestros servicios), comunicar, publicar, desplegar o mostrar públicamente y distribuir dicho contenido. Google usará los derechos que le confiere esta licencia únicamente con el fin de proporcionar, promocionar y mejorar los Servicios y de desarrollar servicios nuevos". Disponible en: <https://www.google.com/intl/es/policies/terms/>. [Fecha de consulta: 10 de agosto de 2016].

88 Es el caso del servicio *cloud* de plataforma SAP Hana, que se compromete a usar los contenidos únicamente para la provisión del servicio, aunque los téminos de la licencia son bastante amplios, ya que permiten reproducir, adaptar, modificar, traducir, publicar, ejecutar públicamente y distribuir esos contenidos: *"By submitting, posting or displaying your application or other content or data (including content or data provided by end users) ("your content") on or through the service, You hereby grants SAP a worldwide, sublicensable, non-transferable, non-exclusive, terminable, limited license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute your content for the sole purpose of enabling SAP to provide You with the service in accordance with this agreement".* Condiciones del servicio SAP Hana [en línea]. Disponibles en: <https://accounts.sap.com/ui/public/viewTextResource?scenario=SAP_HANA_Cloud_Developer_Edition&resourceType=RESOURCE_TERMS_OF_USE&locale=en_US&spDisplayName=SAP%20

ocasiones estas licencias de uso pueden abarcar finalidades más abiertas, como fines publicitarios o promocionales. Tras examinar algunas de las redacciones, sobre todo en aquellas incluidas en condiciones generales de software como servicios gratuitos o enfocados a consumidores, o en términos de uso de redes sociales, observamos que pueden comprender incluso la aceptación para usos comerciales por parte del proveedor o sus socios o filiales[89]. Es importante, a nuestro parecer, que se valoren los potenciales posibles usos de la obra que el proveedor se reserva, y que, en caso de duda, se interprete esta licencia de manera restrictiva y en beneficio del licenciante, teniendo en cuenta su posición de adherente y la imposibilidad de negociación de tales licencias.

Frecuentemente, el beneficiario de la licencia no solo resulta ser el proveedor

---

HANA%20Cloud%20Developer%20Edition>. [Fecha de consulta: 10 de agosto de 2016].

89 Veamos este ejemplo de cláusula recogida en las condiciones generales del proveedor Google, aplicables a todos sus productos y servicios: "Algunos de nuestros servicios te permiten subir, enviar, almacenar o recibir contenido. Si lo haces, seguirás siendo el titular de los derechos de propiedad intelectual que tengas sobre ese contenido. En pocas palabras, lo que te pertenece, tuyo es". Sin embargo, a continuación, en la misma cláusula del mismo contrato, el cliente está cediendo una serie de facultades a Google sobre los contenidos, sin especificar si estos contenidos son o no susceptibles de generar derechos de propiedad intelectual: "Al subir, almacenar o recibir contenido o al enviarlo a nuestros servicios o a través de ellos, concedes a Google (y a sus colaboradores) una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas (por ejemplo, las que resulten de la traducción, la adaptación u otros cambios que realicemos para que tu contenido se adapte mejor a nuestros servicios), comunicar, publicar, ejecutar o mostrar públicamente y distribuir dicho contenido. Google usará los derechos que le confiere esta licencia únicamente con el fin de proporcionar, promocionar y mejorar los servicios y de desarrollar servicios nuevos. Esta licencia seguirá vigente incluso cuando dejes de usar nuestros servicios (por ejemplo, en el caso de una ficha de empresa que hayas añadido a Google Maps)". Como vemos en estas condiciones de Google, además de no hacer distinciones entre contenidos que puedan ser objeto o no de protección legal (por la legislación sobre propiedad intelectual, por ser secretos de empresa, etc.) el proveedor se reserva el derecho a usar, modificar y distribuir los contenidos migrados del cliente, aunque bajo el compromiso únicamente de suministro, promoción o mejora de los servicios de Google (lo cual puede ser, como podemos deducir, objeto de interpretaciones bastante flexibles al tratarse de conceptos indeterminados). En nuestra opinión, una licencia tan amplia y tan poco delimitada tanto en su objeto como en su duración nos parece susceptible de ser considerada abusiva de acuerdo con el art. 82.1 de la Ley General para la Defensa de los Consumidores y Usuarios (Art. 82.1 TRDCU: "Se considerarán cláusulas abusivas todas aquellas estipulaciones no negociadas individualmente y todas aquellas prácticas no consentidas expresamente que, en contra de las exigencias de la buena fe causen, en perjuicio del consumidor y usuario, un desequilibrio importante de los derechos y obligaciones de las partes que se deriven del contrato"). Sin embargo, la pequeñas empresas que suscriban estas condiciones tendrán más dificultades para evitar su aplicación, al quedar fuera del amparo del control de contenidos de las condiciones generales. Extracto de las condiciones generales de uso de los servicios de Google [en línea]. Disponible en: <https://www.google.com/intl/es/policies/terms/>. [Fecha de consulta: 2 de mayo de 2017].

cloud con quien se suscribe el contrato, sino que esta licencia se amplía a terceros con quienes aquel colabora para ofrecer la prestación. Para dar flexibilidad a la cobertura de la autorización, las menciones a estos terceros se realizan con expresiones genéricas, como "nosotros", "nuestros afiliados"[90] o "nuestros colaboradores"[91]. Algunos de estos beneficiarios efectivamente actuarán como licenciatarios para garantizar la adecuada prestación del servicio, como por ejemplo los subcontratistas de capas inferiores de la arquitectura *cloud* o las filiales que facilitan el suministro del servicio en otros territorios. No obstante, yendo más allá, la amplia redacción de cláusulas de este tipo podría incluso acoger a socios comerciales, lo cual abriría la posibilidad de una autorización para usos lucrativos de los contenidos del usuario, renunciando este, a través de la suscripción de las condiciones generales, a cualquier remuneración o reclamación de derechos mediante la concesión previa de esta licencia[92]. Si fuera así, esta cláusula es

90 Por ejemplo, el servicio de plataforma gratuito *Force.com* del proveedor *cloud* Salesforce nos habla de *affiliate*, que define como filiales: "You grant us and our affiliates a worldwide, limited- term license to host, copy, transmit and display your Data, and any non-Salesforce.com applications and program code created by or for you using a service, as necessary for us to provide the services in accordance with this agreement. Subject to the limited licenses granted herein, we acquire no right, title or interest from you or your licensors under this agreement in or to your data or any non-Salesforce.com application or program code. (…) "Affiliate" means any entity which directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity". Términos del servicio *Force.com* [en línea]. Disponible en: <http://www.sfdcstatic.com/assets/pdf/misc/forcedotcom_Free_Edition_Agreement.pdf*>.* [Fecha de consulta:2 de mayo de 2017].

91 Así aparece en la redacción de las condiciones generales comunes a todos los productos y servicios de Google [en línea]. Disponible en: <https://www.google.com/intl/es/policies/terms/>. [Fecha de consulta: 2 de mayo de 2017].

92 La licencia que el usuario concede a la red social Facebook sobre sus contenidos objeto de derechos de propiedad intelectual, viene configurada como "transferible" y "con posibilidad de ser subotorgada" en la propia cláusula. Esta libertad de transferencia permitiría su cesión o su venta, incluso de forma remunerada, a terceros que pudiesen explotarla, sin que el usuario tuviese derecho a reclamación alguna: "Eres el propietario de todo el contenido y la información que publicas en Facebook y puedes controlar cómo se comparte a través de la configuración de la privacidad y de las aplicaciones. Además, en relación con el contenido con derechos de propiedad intelectual (contenido de PI), como fotos y vídeos, nos otorgas específicamente el siguiente permiso, sujeto a tu configuración de la privacidad y de las aplicaciones: nos otorgas una licencia no exclusiva, transferible, con posibilidad de ser subotorgada, libre de regalías y aplicable globalmente para utilizar cualquier contenido de IP que publiques en Facebook o en conexión con Facebook (licencia de PI)". En su política de privacidad, reconoce que terceros pueden recibir información sobre los contenidos publicados: "aplicaciones, sitios web o otros servicios de terceros que utilizan nuestros servicios". Además, puede compartirse "la información que tenemos sobre ti" dentro del "grupo de empresas de Facebook" y con "colaboradores externos", que

susceptible de considerarse abusiva.

Por otra parte, en la regulación contractual de los servicios de computación en la nube, la fijación del plazo de duración de las licencias no es uniforme. Así, existen licencias con una duración determinada (por ejemplo, con vigencia equivalente a la duración de la relación contractual), con un plazo indefinido o sin especificación del plazo[93]. Es interesante que el licenciante valore las concesiones que impliquen plazos especialmente amplios, siendo recomendable que la licencia concedida se extinga en el momento en el cual se termine la relación contractual entre proveedor *cloud* y cliente.

No se establece contraprestación por las licencias de uso que concede el usuario al proveedor. Ello tiene sentido porque muchos de estos usos son preceptivos para un adecuado suministro del servicio, como la compartición de contenidos con otros usuarios, la realización de copias y replicado de contenidos por razones de seguridad y resiliencia, el almacenamiento remoto de información en servidores que

---

incluyen "servicios de publicidad, medición y análisis" que pueden realizar tareas de extracción de datos (data mining) y "proveedores generales, de servicios y otros socios" sujetos a acuerdos de confidencialidad. Con la concesión de este tipo de licencias, la única limitación legal para la explotación de los contenidos del usuario es la cobertura por secreto de empresa, y aquellas obligaciones que sean aplicables en materia de protección de datos personales, pero se está renunciando a cualquier derecho sobre propiedad intelectual sobre lo que se comparte. A nuestro parecer, este tipo de licencias deberían considerarse abusivas, puesto que imponen una privación de derechos injustificada e innegociable en perjuicio de los intereses del usuario, y tras la que puede esconderse un afán de lucro por parte del proveedor, puesto que el proveedor en ningún momento se compromete a no realizar explotaciones comerciales de los contenidos. Condiciones de la red social Facebook y FAQs (*Frequently Asked Questions*) sobre usos de contenidos del usuario [en línea]. Disponible en: <https://www.facebook.com/legal/terms/update>; y <https://es-es.facebook.com/about/privacy/>. [Fecha de consulta: 2 de mayo de 2017].

93 Facebook establece, para la licencia de uso que concede el usuario sobre sus contenidos, una duración vinculada al borrado de los contenidos de la cuenta, con lo cual, si se tiene en cuenta la persistencia de obras objeto de derechos de autor que se han compartido y publicado dentro del servicio, la duración de la licencia puede resultar imposible de delimitar. "Esta licencia de PI [propiedad intelectual] finaliza cuando eliminas tu contenido de PI o tu cuenta, salvo si el contenido se ha compartido con terceros y estos no lo han eliminado". Tengamos en cuenta, además, como funciona el mecanismo de borrado en la nube (ver capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube"), que como las misma cláusula de Facebook indica: "cuando eliminas contenido de PI [propiedad intelectual], este se elimina de forma similar a cuando vacías la papelera de reciclaje de tu ordenador. No obstante, entiendes que es posible que el contenido eliminado permanezca en copias de seguridad durante un plazo de tiempo razonable (si bien no estará disponible para terceros)". Condiciones de uso de Facebook [en línea]. Disponible en: <https://es-es.facebook.com/legal/terms?locale=es_ES>. [Fecha de consulta: 2 de mayo de 2017].

pueden pertenecer a terceros, etc.

En cuanto a los usos no necesarios para la prestación, pero que igualmente el usuario haya consentido mediante la licencia, el proveedor no se suele someter a ninguna obligación de rendir cuentas al titular de los datos sobre los usos licenciados, ni tampoco se compromete a compensarle por tales usos. Por ello es necesario que el suscriptor valore esta posibilidad cuando contrate el servicio cloud. Por otra parte, puede entenderse que los beneficios que obtiene el usuario gracias a las funcionalidades *cloud* hacen las veces de contraprestación en aquellos casos en los cuales el servicio se presta sin contraprestación dineraria del cliente[94]. Sin embargo, nada impide al usuario establecer reclamaciones por usos de contenidos que sobrepasen las actividades necesarias para el funcionamiento y prestación adecuada del servicio, especialmente en aquellos casos en los que el proveedor obtenga un considerable lucro o infrinja derechos morales del autor (y, por tanto, irrenunciables según el art. 14 TRLPI)[95].

Finalmente, aunque es habitual que estas licencias se concedan sin delimitación geográfica, por tratarse de servicios comercializados globalmente, cabe destacar que no todas las licencias de uso serán igualmente válidas en todos los países. Por ejemplo, las inversiones realizadas en la creación de bases de datos carecen de protección en ciertos países en los que rige el sistema anglosajón. Será importante determinar la legislación aplicable de acuerdo con el Derecho Internacional Privado para saber si realmente existen derechos de autor sobre la obra, quién ostenta su titularidad o si se han infringido a través de alguna actuación o uso ilícito.

94 La Propuesta de Directiva de suministro de contenidos digitales no trata cuestiones relacionadas con los derechos de autor y otros derechos de propiedad intelectual, tal y como se recoge en su considerando 21, con lo cual no tendrá incidencia en las licencias contenidas en las condiciones contractuales: "La presente Directiva no debe tratar sobre derechos de autor o sobre otros aspectos relacionados con derechos de propiedad intelectual del suministro de contenidos digitales. Por tanto debe entenderse sin perjuicio de los derechos y obligaciones en virtud de la legislación sobre derechos de autor y otras leyes de propiedad intelectual".

95 En relación a los servicios ofertados como "gratuitos" para el usuario, cabe mencionar que la gratuidad debería entenderse en estos casos como falta de contraprestación de carácter económico, porque pueden existir otras remuneraciones no pecuniarias en favor del proveedor o de terceros (otros usuarios o colaboradores del proveedor), como cesiones de derechos de propiedad intelectual, recepción de envíos de publicidad no solicitada, autorizaciones para usos o cesiones de datos de carácter personal a terceros, etc.

4.2.2.- Los contenidos titularidad de un tercero migrados a la nube por un usuario. El caso especial del software y las bases de datos

Cuando los contenidos que tengan consideración de obra de acuerdo con la normativa de propiedad intelectual no son creación del usuario, este, como se ha dicho, podrá realizar algunos usos, como actos de mero acceso a la obra y descargas de la obra en dispositivos de almacenamiento propios (siendo este un acto de copia privada según el art. 31.2 TRLPI)[96]. En cambio, podrá llevar a cabo actos de explotación únicamente cuando sea beneficiario de algún tipo de licencia o autorización del titular de los derechos de propiedad intelectual que le permita el uso de la obra en formato digital[97].

Cuando el usuario accede lícitamente a una obra o la adquiere en formato digital (por ejemplo, a través de una tienda *online* que permite la descarga[98]),

96 No necesitará autorización del titular de los derechos cuando se encuentre en alguna de las situaciones legales comprendidas en los art. 31 a 40 del TRLPI. Algunos ejemplos de limitaciones al derecho de autor recogidas en estos artículos son, entre otros, la copia de la obra para uso personal y sin ánimo de lucro (excepto programas de ordenador y bases de datos electrónicas), los usos en contextos educativos o las parodias.

97 XALABARDER PLANTADA, Raquel; "Redes sociales...", *op. cit.*, pág. 345.

98 Veamos, aunque no sea un contrato de computación en la nube, la cláusula de las condiciones particulares para la venta de libros electrónicos de la tienda en línea La casa del Libro, que concede la licencia de uso de libros en formato digital, a título ilustrativo: "El cliente reconoce que la compañía le concede una licencia para utilizar los *eBooks* comercializados por la compañía. Una vez adquirida, dicha licencia consistirá en una relación contractual directa entre el cliente y el tercero proveedor de los contenidos digitales en cuestión, esto es "el editor". El editor de cada *eBook* es responsable de su contenido, de las garantías, en su caso, y de cualesquier reclamación que el/los cliente/s o cualquier tercero puedan realizar en relación con dicho *eBook*". Además, las mismas condiciones restringen el uso concedido: "Restricciones de Uso. 1. El cliente únicamente utilizará los *eBooks* para fines particulares y no comerciales. La licencia de uso de los *eBooks* no supone una transmisión de ningún derecho de uso con fines promocionales. Entre otras cuestiones, está expresamente prohibido al cliente: vender, alquilar, prestar, realizar copias, modificar, transformar, distribuir y/o poner a disposición del público los *eBooks*, ya sea parcialmente, ya sea en su totalidad, de cualquier forma que no esté expresamente permitida en las presentes condiciones particulares; eliminar, modificar, suprimir o cualquier forma similar de impedir el efectivo funcionamiento de cualquier medida adoptada para evitar la copia, distribución, puesta a disposición del público, modificación, transformación o cualquier otro tipo de acceso o tratamiento indebido o no autorizado de los *eBooks*, ya sea parcialmente, ya sea en su totalidad; facilitar o compartir el nombre de usuario y contraseña con cualquier tercero distinto del usuario; burlar cualquier tecnología utilizada para proteger los *eBooks* accesibles a través de la web de Casa del Libro, así como suprimir o eliminar de los *eBooks* cualquier mención o referencia al aviso de los derechos sobre los mismos; utilizar los *eBooks* de cualquier forma que implique un incumplimiento de las presentes condiciones particulares". Condiciones del contrato de compraventa de *eBooks* de la tienda *online* La Casa del Libro [en línea]. Disponible en: <http://www.casadellibro.com/ayuda/condicionesContratacion>. [Fecha de consulta: 2 de mayo de 2017].

realmente no está adquiriendo la propiedad de la copia, sino el uso personal de esta copia, con lo cual este uso puede limitarse a través de la licencia[99].

Según la doctrina, el acto de "subir" a Internet obras de titularidad de un tercero implica, cuando la obra sale por primera vez a la luz, un acto de divulgación, y, en la medida en que esa obra se pone a disposición del público en general, los actos de reproducción y comunicación pública[100]. Así las cosas, el almacenamiento remoto en sistemas de computación en la nube sería susceptible de considerarse una actividad de reproducción (art. 18 TRLPI[101]), puesto que generalmente lo que se almacena es una copia de la obra, aunque esta copia resultaría necesaria para la prestación del servicio, ya que se efectúa por motivos de seguridad o resiliencia. Por otra parte, la carga de obras digitales en Internet cuando estas sean accesibles a terceros se considera un acto de puesta a disposición, con lo cual se estará realizando este acto cuando el uso de los servicios *cloud* implique compartir y publicar obras en Internet[102].

Los actos de reproducción y puesta a disposición deberán tenerse en cuenta especialmente en aquellos servicios *cloud* que permitan compartir o publicar contenidos, cuando estos contenidos sean susceptibles de considerarse obras con derechos de propiedad intelectual[103]. Si el uso de la copia digital (obtenida

99 ÁLVAREZ, Henar; "Aspectos jurídicos de las descargas de música en Internet", *Nuevos retos para la propiedad intelectual: II Jornadas sobre la Propiedad Intelectual y el Derecho de Autor/a*, (coord. Rafael García Pérez, Marcos A. López Suárez), La Coruña, 2008, pág. 104.

100 XALABARDER PLANTADA, Raquel; "Redes sociales...", *op. cit.*, pág. 344. BAYLINA MELÉ, Marta. "La explotación directa de obras y prestaciones protegidas en redes digitales", *Novedades en la Ley de Propiedad Intelectual,* 1ª edición, Barcelona, 2007, pág. 27. Ver también APARICIO VAQUERO, Juan Pablo, "Propiedad Intelectual y suministro de contenidos digitales" [en línea], *Revista InDret para el análisis del Derecho*, núm. 3, 2016. Disponible en: <http://www.indret.com/pdf/1242.pdf>. [Fecha de consulta: 1 de junio de 2017].

101 Art. 18 TRLPI: "Se entiende por reproducción la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda la obra o de parte de ella, que permita su comunicación o la obtención de copias".

102 Arts. 20.1 y 20.2 del TRLPI: "Se entenderá por comunicación pública todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas. (...). Especialmente, son actos de comunicación pública: (...) i) La puesta a disposición del público de obras, por procedimientos alámbricos o inalámbricos, de tal forma que cualquier persona pueda acceder a ellas desde el lugar y en el momento que elija".

103 Existe el debate sobre si algunos contenidos digitales son susceptibles de ser considerados "obras" en el sentido legal de la palabra y como objeto digno de ser protegido jurídicamente. Se plantea esta cuestión en relación con los *tweets*, mensajes que, con un máximo de 140 caracteres,

lícitamente[104]) es privado y no colectivo ni lucrativo, será lícito[105]. No entraría en estos supuestos de uso lícito de la copia digital la puesta a disposición del público de la obra para su descarga o uso en perjuicio del autor y de sus derechos de explotación, como puede ser la publicación de su enlace en sitios web *peer to peer*, o permitir la descarga de la obra al público en general sin autorización ni

---

se crean, publican y comparten por usuarios de la red social Twitter. Si bien son creación intelectual de una persona física, a quien llamaríamos autor, su brevedad puede originar dudas sobre la existencia de una obra realmente original y de una altura creativa suficiente como para ser objeto de una protección jurídica equiparable a la de otras obras de creación intelectual. Aun teniendo en cuenta estas consideraciones, se ha dado el caso de que la editorial Larousse ha retirado del mercado el libro *Perles des Tweet et du Net* (*Perlas de los tweets y de la red)*, un compendio de estos mensajes y de otros comentarios publicados en distintas webs 2.0, principalmente porque en el libro no se recababa la autorización de los autores de las publicaciones ni se reconocía su derecho de paternidad. Al tratarse de un uso lucrativo de estos mensajes obtenidos sin autorización, susceptibles de ser considerados obras, y previendo posibles demandas judiciales, la editorial ha retirado los ejemplares del mercado. A nuestro parecer, el principal error de la editorial no fue captar estos mensajes y publicarlos, sino la falta de autorización de sus autores en cuanto al uso lucrativo de sus mensajes y su reconocimiento como autores de esos *tweets*. Otro aspecto que sería relevante en cuanto a la legalidad de su actuación, a nuestro parecer, es si la editorial Larousse obtuvo esos contenidos a través de una cuenta de usuario o gracias a un acuerdo consentido con el propio proveedor de contenidos Twitter, para saber si este uso lucrativo entraba o no en contradicción con los términos de uso de la propia red social. Así, si hubiera mediado acuerdo entre editorial y red social, la reclamación por parte de usuarios se hubiera complicado, al haber consentido el usuario con esta condición general: "Usted acepta que este permiso otorga el derecho a Twitter de proporcionar, promover y mejorar los servicios y de poner a la disposición de otras compañías, organizaciones o individuos asociados con Twitter el contenido presentado a través de los servicios para la sindicación, difusión, distribución o publicación de dicho contenido en otros medios y servicios, según nuestros términos y condiciones para utilizarlo" y que "Twitter y otras compañías, organizaciones o personas asociadas con Twitter podrán llevar a cabo tales usos adicionales sin compensarlo de ninguna manera por el contenido que usted envíe, publique, transmita o ponga a disposición a través de los servicios". Fuentes de la noticia*:* GUIX TORNOS, Anna; "Redes sociales y derechos de autor: ¿de quién son los contenidos?"*, Actualidad jurídica Aranzadi*, núm. 879, Navarra, 2014, pág. 8. CZARNY, Raphäel; "Comment Larousse a oublié la propriété intellectuelle des utilisateurs de Twitter" [en línea], *Slate Magazine,* 2014. Disponible en: <http://www.slate.fr/story/82495/twitter-larousse-propriete-intellectuelle>. [Fecha de consulta:2 de mayo de 2017].

104 Es decir, que su acceso no ha tenido lugar violando medidas de seguridad de bases de datos o copias no autorizadas de soportes físicos.

105 La compartición de los contenidos de copia privada con otros usuarios de la nube, autorizados e identificables por el tenedor lícito de la copia privada, queda amparada, a nuestro parecer, por la normativa de propiedad intelectual, del mismo modo en que un compañero puede prestarnos un libro o adjuntárnoslo en formato PDF en un correo electrónico. Para paliar el perjuicio económico que estas copias privadas ocasionan al autor, se estableció en el artículo 25 del Texto Refundido de la Ley de Propiedad Intelectual la compensación equitativa por copia privada.

remuneración al autor o al titular de los derechos[106]. Lo anterior rige siempre y cuando no se trate de programas de ordenador o bases de datos (art. 31.2 LPI), en cuyo estudio nos detendremos más adelante[107].

Por otro lado, el disfrute de la obra licenciada puede tener una duración temporal (por ejemplo, al permitir la escucha de una canción a través de *streaming*[108]) o ser duradero (al permitir una descarga en el disco duro del usuario o en un sistema de almacenamiento en la nube)[109]. Trasladando estas autorizaciones al contexto de la nube, y dependiendo del eventual mecanismo que el usuario haya utilizado para la descarga digital de estos contenidos, se permitirán su descarga y almacenamiento tanto en soportes virtuales remotos como en diferentes dispositivos físicos del usuario que ha adquirido la obra legítimamente[110], sin que ello afecte a la prohibición general de utilizar esa copia digital, inicialmente obtenida para su disfrute privado, de forma lucrativa o colectiva (art. 31.2 de la LPI)[111].

---

106 XALABARDER PLANTADA, Raquel; "Redes sociales...", *op. cit.*, pág. 346.

107 Art. 31. 2 del Texto Refundido de la Ley de Propiedad Intelectual: "No necesita autorización del autor la reproducción, en cualquier soporte, de obras ya divulgadas cuando se lleve a cabo por una persona física para su uso privado a partir de obras a las que haya accedido legalmente y la copia obtenida no sea objeto de una utilización colectiva ni lucrativa, sin perjuicio de la compensación equitativa prevista en el artículo 25, que deberá tener en cuenta si se aplican a tales obras las medidas a las que se refiere el artículo 161. Quedan excluidas de lo dispuesto en este apartado las bases de datos electrónicas y, en aplicación del artículo 99.a), los programas de ordenador".

108 Entendemos el concepto *streaming* como la visualización de contenidos digitales de vídeo o audio a través de la conexión a Internet, de manera fluida y sin interrupciones (del término inglés *stream*: corriente que fluye de manera continua) sin necesidad de descargarlos completamente en el equipo informático del receptor para poder acceder a su contenido. (Definición propia).

109 ÁLVAREZ, Henar; "Aspectos jurídicos de las descargas de música en Internet", *Nuevos retos para la propiedad intelectual: II Jornadas sobre la Propiedad Intelectual y el Derecho de Autor/a*, (coord. Rafael García Pérez, Marcos A. López Suárez), La Coruña, 2008, pág. 104.

110 El art. 31.2 del TRLPI establece como fuentes lícitas, a efectos de copia privada: "A estos efectos, se entenderá que se ha accedido legalmente y desde una fuente lícita a la obra divulgada únicamente en los siguientes supuestos: 1.º Cuando se realice la reproducción, directa o indirectamente, a partir de un soporte que contenga una reproducción de la obra, autorizada por su titular, comercializado y adquirido en propiedad por compraventa mercantil. 2.º Cuando se realice una reproducción individual de obras a las que se haya accedido a través de un acto legítimo de comunicación pública, mediante la difusión de la imagen, del sonido o de ambos, y no habiéndose obtenido dicha reproducción mediante fijación en establecimiento o espacio público no autorizada".

111 Por ejemplo, nada impide que un usuario que ha adquirido legítimamente un disco de música en formato físico, digitalice su contenido en formato MP3 y lo almacene en un software como servicio (SaaS) de almacenamiento tipo Dropbox. En cambio, cuando se adquiere una obra literaria para su descarga y lectura electrónica en dispositivos tipo *e-book,* en ocasiones se obtendrá una copia en formato PDF de la obra (lo cual permitirá su almacenamiento en la nube), y

En resumen, no se permite, salvo autorización expresa del titular, la comunicación pública o la explotación comercial de obras digitales que sean objeto de derechos de autor, ya sea en su uso fuera de la nube como una vez migrada por el usuario, aunque sí su uso privado. Por último, cabe mencionar que no será necesaria la autorización del autor cuando los contenidos ya pertenezcan al dominio público o corresponda a una excepción a la autorización del titular de los artículos 31 y siguientes del TRLPI[112].

---

en otras se permitirá el acceso a la obra a partir de ciertos dispositivos o se permitirá un número limitado de accesos a la obra en *streaming* (con lo cual no será posible almacenar tales obras en la nube porque no se habrá podido descargar una copia en formato digital). Veamos un ejemplo de esta posibilidad a través de una cláusula de las condiciones particulares de la tienda en línea La casa del Libro, para la compra de libros electrónicos, en los que se informa al usuario de cómo puede acceder a la obra literaria en formato electrónico para leerla: "Para la lectura de *eBooks* el cliente tendrá 3 modalidades para acceder a los mismos: [1ª.-] El acceso off-line mediante descarga inmediata de la web de Casa del Libro en *ePub Adobe DRM*, limitado a un máximo de 3 descargas en dispositivos de lectura compatibles con el programa *Adobe Digital Editions*. [2ª.-] El acceso *off-line* mediante descarga en formato *ePub* TAGUS de Casa del Libro hasta en un máximo de 5 dispositivos compatibles (*Ipad, Iphone, Tablet Android*, *Smarphone Android*) registrados previamente. En este caso el cliente deberá registrar en el apartado correspondiente en la web los dispositivos en los que realice la/s descarga/s. Podrá cambiar los dispositivos siempre que lo crea oportuno con la limitación de tener únicamente 5 dispositivos dados de alta y un máximo de 3 cambio al mes. El acceso *off-line* mediante descarga de *ePub* en formato *Adobe DRM* y *ePub* en formato TAGUS de Casa del Libro, tiene la limitación de 6 descargas en total por *eBook* comprado sumando las descargas en uno y otro formato. [3º.-]. El acceso *on-line*. Este formato permite al cliente la lectura del *eBook* en su biblioteca digital situada en la web de Casa del Libro a través de un navegador de Internet de los indicados como compatibles. Para la lectura *on-line* no se permitirá la concurrencia, únicamente se permitirá una lectura simultanea de un mismo *eBook* y de un solo dispositivo. El cliente podrá realizar la lectura *on-line* siempre que lo requiera en *streaming* desde cualquier dispositivo compatible a través de navegadores compatibles indicados en la web casadellibro.com". Condiciones de contratación del sitio web La Casa del Libro [en línea]. Disponible en: <http://www.casadellibro.com/ayuda/condicionesContratacion> [Fecha de consulta: 2 de mayo de 2017.

112 Las obras entran en dominio público cuando termina el periodo de vigencia del derecho de autor concedido por la TRLPI. Por ejemplo, una obra compuesta por Mozart, una reproducción de un texto de Bécquer o una imagen de un cuadro de Edward Munch. Sin embargo, sí estarán protegidas las obras de nuevos autores derivadas de obras en dominio público y las interpretaciones u otras actividades susceptibles de generar derechos conexos. Del mismo modo, las excepciones legales a la necesidad de autorización del autor responden a distintas justificaciones (interés general, libertad de expresión, docencia e investigación, etc.), y se recogen en una lista cerrada, en los arts. 31 y siguientes del TRLPI. A modo de ejemplo: obras que afecten a informaciones sobre acontecimientos de la actualidad (art. 35.1 TRLPI), fotografías de obras situadas en la vía pública (art. 35.2 TRLPI), citas o reseñas (art. 32.1 TRLPI) o la ya mencionada excepción de copia privada (art. 31.2 TRLPI). XALABARDER PLANTADA, Raquel; "Redes

Sin perjuicio de lo anterior, debemos tener en cuenta los nuevos formatos de licencias que permiten la autogestión del autor de sus derechos de propiedad intelectual, dada la generalización de la puesta a disposición del público de obras por parte de sus autores que cuelgan sus trabajos en Internet. Nos referimos a las denominadas licencias abiertas, como las licencias *Creative Commons*, concebidas para todo tipo de obras. A diferencia de lo que ocurre con las licencias tradicionales, mediante las licencias abiertas el titular de los derechos autoriza a terceros su copia, modificación o distribución, según las indicaciones de los iconos estándares publicados junto con la obra[113]. Son muy comunes en el ámbito literario y musical, porque, entre otras razones, su circulación sin demasiadas restricciones a través de la Red facilita la promoción y divulgación de obras, en ocasiones conveniente a efectos de marketing viral y entrada en el mercado de un nuevo autor.

El software y los derechos que de este pueden derivarse, así como su licencia en la nube, merece mención aparte del resto de obras. El TRLPI dedica al software específicamente el Título VII, de manera separada. Ello se debe a que, al adquirir el software, no se adquiere un producto, sino que se obtiene una licencia mediante la cual se permite al licenciatario ejecutar ese programa informático bajo varias condiciones. El licenciante, por su parte, se reserva para sí otros derechos, entre ellos la facultad de otorgar más licencias sobre ese software o la posibilidad de modificar o actualizar sus contenidos o funcionalidades. Todo lo anterior sucede cuando se trata del denominado software propietario, en el cual el titular de los derechos autoriza a un tercero su utilización. Por tanto, algunas restricciones habituales en las licencias de uso no personalizadas de software pueden ser relevantes a la hora de utilizar ese software en entornos de la nube.

---

sociales...", *op. cit.*, págs. 347-348.

113 Estos iconos visuales representan cada uno de los derechos cedidos o reservados por el autor. Las seis modalidades de licencias *Creative Commons* son el resultado de la combinación de cuatro condiciones (reconocimiento de la autoría, limite a usos no comerciales, prohibición de realización de obras derivadas y obligación de conservación de las condiciones de licencia al divulgarse la obra), que el autor puede configurar para cada una de sus obras que se pongan a disposición del público en la Red. Para más información sobre las licencias *Creative Commons*, puede visitarse su página web oficial para España. Disponible en: <http://es.creativecommons.org/blog/cc-es/>. [Fecha de consulta: 2 de mayo de 2017]. Para un detallado análisis jurídico, nos remitimos a XALABARDER PLANTADA, Raquel (2006). "Las licencias Creative Commons: ¿una alternativa al *copyright*?" [en línea], *UOC Papers,* núm. 2, Universitat Oberta de Catalunya, 2006. Disponible en: <http://www.uoc.edu/uocpapers/2/dt/esp/xalabarder.pdf>. [Fecha de consulta: 2 de mayo de 2017].

A modo de ejemplo, debe prestarse especial atención a las restricciones de la licencia que hacen mención a su uso en un ordenador determinado, a una localización geográfica determinada o limitada, en un número determinado de equipos físicos, a su uso únicamente por la persona del propio licenciatario, o a la confidencialidad de ese programa o de sus contenidos. Dependiendo de la concreta redacción de las cláusulas de la licencia, puede entenderse que no se permite su ejecución en entornos virtualizados, ni su alojamiento en servidores remotos, en los cuales se pueda acceder por terceros al software propietario (lo cual puede incluir al proveedor *cloud,* susceptible de ser considerado tercera parte que puede tener acceso a ese software)[114].

Frente a las licencias tradicionales de software se encuentran las llamadas licencias de código abierto, promovidas, entre otras organizaciones, por la *Open Source Iniciative*[115]*.* Estas licencias de software son menos restrictivas que las tradicionales de derechos de autor, puesto que permiten la libre redistribución y la posibilidad de realizar obras derivadas. Su finalidad es facilitar a los desarrolladores la mejora del programa informático, y para ello se publica o se pone a disposición de los desarrolladores interesados el código fuente.

Una característica de las licencias de código abierto es la exigencia de que cuando el software de código abierto se distribuye posteriormente por el licenciatario, debe permitirse la libre redistribución, es decir, que ese software pueda ser vendido o accedido por terceros libremente, y se permitirán obras derivadas del software original y del programa o programas que sean resultado de modificaciones. Todo ello trata de conseguir el efecto viral de ese software y permitir su constante desarrollo, mejora y actualización, sin que un usuario pueda paralizar la cadena y entorpecer ese fin[116]. Por ello, el uso de software de código abierto tanto por proveedores *cloud* que lo ponen a disposición de sus usuarios (software de virtualización, software del almacenamiento de archivos, y otro software a nivel de

114 MARCHINI, Renzo; *Cloud Computing: A practical introduction to the legal issues,* 1ª edición, Londres, 2010, pág. 91.

115 Para considerarse licencias *Open Source* o de código abierto, la *Open Source Iniciative* establece determinados requisitos, como el acceso al código fuente, la libre redistribución, la autorización de realizar trabajos derivados sobre el programa original, etc. Para más información sobre estas licencias, nos remitimos al sitio web de la *Open Source Iniciative*. Disponible en: <https://opensource.org/>. [Fecha de consulta: 2 de mayo de 2017].

116 MARCHINI, Renzo*, op. cit.,* págs. 93, 94.

infraestructura y plataforma), como de usuarios desarrolladores que lo migran, utilizan y mejoran en plataformas *cloud*, deben tener en cuenta esta consideración antes de volver a distribuirlo o comercializar el nuevo programa basado en el anterior software de código abierto. De lo contrario, estarán infringiendo la licencia que les permite su uso legítimo.

Si estas licencias de código abierto cumplen una serie de requisitos pueden considerarse software libre, como sucede con las licencias GNU GPL[117]. El software libre permite, como su propio nombre indica, muchas libertades que normalmente el titular de derechos del software propietario no concede[118]. El software libre, una vez adquirido (con o sin remuneración), permite, a través de su licencia, su libre uso, análisis, copia, modificación y distribución tanto de la copia original como de su copia transformada, de modo que toda la comunidad (privada, educativa, pública, militar, etc.) pueda beneficiarse de estas mejoras que necesitan, para poder realizarse, el acceso al código fuente[119].

---

117 Cabe mencionar que, además de las diferencias prácticas, tras la elección entre las licencias de código abierto o libre subyacen fundamentos filosóficos, éticos e ideológicos distintos, en cuyo estudio no nos adentraremos en este trabajo. La GNU GPL o Licencia Pública General del Proyecto *GNU* posibilita la redistribución y modificación del software, pero con la condición que el software resultante se someta al mismo tipo de licencia de software libre, aunque se haya mezclado con otro software o códigos sujetos a licencias más estrictas, con lo cual el programador que las use debe estar atento a la compatibilidad entre licencias. Para más información sobre la compatibilidad entre licencias libres, se recomienda visitar la web oficial de GNU. <http://www.gnu.org/licenses/license-list.html#SoftwareLicenses>. [Fecha de consulta: 2 de mayo de 2017].

118 La principal impulsora del software libre es la *Free Software Foundation*. Esta fundación ha creado una licencia para software que se ejecuta a partir de una red de ordenadores, denominada *Affero GPL*, que añade a la licencia GNU GPL la obligación de distribuir ese software que se ejecuta para ofrecer servicios a través de una red de ordenadores. Para más información, nos remitimos a su sitio web, disponible en: <https://www.fsf.org>, [Fecha de consulta: 2 de mayo de 2017], y a MARCHINI, Renzo*, op. cit.,* pág. 95.

119 A consecuencia de una inadecuada traducción, en ocasiones el *free software* (software libre) se traduce como software gratuito (también denominado *freeware*). Sin embargo, ambos términos no pueden considerarse equivalentes. Ello es así porque aunque en ocasiones el software libre se distribuye de manera gratuita, en otras se ofrece por un mínimo precio que permita cubrir costes. Igualmente, el software gratuito puede no incluir el código fuente y no permitir las libertades en cuanto a modificación y redistribución que el software libre ofrece. Tampoco deben confundirse las licencias de software propietario, de código abierto y software libre con el software de dominio público, que no requiere licencia porque su autor así lo ha decidido o porque hayan expirado los derechos de autor.

A la vista de lo expuesto, podemos concluir que, dependiendo de la licencia adjunta al software que despliegue el usuario en la nube, este estará autorizado a unos u otros usos. Del mismo modo, es habitual encontrar licencias de productos *cloud* con ciertos límites en cuanto a su uso, como por ejemplo la prohibición de migrar ese contenido o su restricción a ciertos dispositivos o por cierto periodo de tiempo[120]. Además de lo anterior, la protección del software realizada por la normativa de propiedad intelectual y por las cláusulas contractuales puede complementarse con otros sistemas de protección legales, como las patentes, los derechos de marca, el deber de confidencialidad y la protección del secreto profesional. Del mismo modo, existen mecanismos técnicos que incrementan la protección tecnológica de dispositivos y programas o métodos especiales de comercialización que protegen el software y otros contenidos digitales de descargas, o copias no autorizadas.

Teniendo en cuenta todas estas cuestiones, queremos adelantar que, en los contratos de computación en la nube examinados para la realización de este trabajo, hemos encontrado prácticamente siempre la exención de responsabilidad del proveedor por contenidos de cualquier índole que puedan suponer infracciones de derechos de propiedad intelectual de terceros y que el usuario haya migrado a su sistema. Estas cláusulas pueden formar parte de la política de uso adecuado (PUA) o aparecer junto con otros contenidos del contrato[121].

---

120 Extracto de la licencia de uso del producto *Microsoft Office 365* [en línea]: "Tu derecho de uso del servicio/software está limitado al periodo de suscripción. Puedes optar por extender tu suscripción, en cuyo caso puedes continuar usando el servicio/software hasta la extinción de este periodo de extensión de la suscripción. (…) Una vez extinguida tu suscripción, la mayoría de funciones del servicio y del software dejarán de estas disponibles. (...) No se permiten las transferencias de licencia. Puedes asignar la licencia de software a otro dispositivo de acuerdo con nuestros derechos de instalación y uso. Cada vez que asignes el software a un nuevo dispositivo, el software dejará de estar disponible para el dispositivo asignado previamente". (Traducción propia). Disponible en: <https://products.office.com/en-us/microsoft-software-license-terms-for-office>. [Fecha de consulta: 2 de mayo de 2017].

121 Aunque el tratamiento jurídico de la responsabilidad de las partes tendrá lugar en un capítulo posterior, adelantamos ahora, simplemente a modo ilustrativo, un ejemplo de estas cláusulas: "Usted acepta NO utilizar el servicio para: (...) e) involucrarse en cualquier infracción de derechos de autor o cualquier otra infracción de propiedad intelectual (incluyendo la carga de cualquier contenido que no tiene derecho a cargar), ni revelar ningún secreto comercial ni información confidencial que infrinja un contrato de confidencialidad, empleo o no revelación". Extracto del contrato de software como servicio de almacenamiento *iCloud* del proveedor Apple [en línea]. Disponibles respectivamente en: <http://www.apple.com/legal/internet-services/icloud/la/terms.html>. [Fecha de consulta: 2 de mayo de 2017]. Asimismo, ver capítulo "Obligaciones y responsabilidades de las partes del

4.3.- Contenidos generados por el usuario dentro del sistema *cloud*

Muchas de las tipologías de servicios que ofrece el *Cloud Computing* permiten al usuario crear contenidos nuevos a partir de las funcionalidades y herramientas de software facilitadas por el proveedor[122]. Inicialmente, la titularidad de estos datos pertenecerá al usuario que los ha creado (en virtud del art. 5 de la LPI[123]). De forma acumulativa, como se ha mencionado, el proveedor deberá garantizar la confidencialidad en relación a ese proyecto, como deber inherente a la naturaleza del contrato[124].

A pesar del principio inicial de atribución de autoría, existen diferentes circunstancias que pueden provocar variaciones, viéndose el usuario privado de su inicial titularidad o limitándose su capacidad de decisión sobre los usos de esos contenidos.

4.3.1.- Creaciones desarrolladas dentro de una relación laboral

Cabe distinguir entre el usuario jurídico de los servicios *cloud*, es decir, el empresario suscriptor, y el usuario material, que puede ser un empleado del suscriptor. Cuando el usuario material de los servicios en la nube tiene una relación laboral con el suscriptor de los servicios, y en concreto en aquellos sectores en los que se encargue un trabajo intelectual a un empleado que pueda dar lugar a una obra susceptible de ser protegida por el TRLPI, es habitual que en el contrato de prestación laboral exista, además de un compromiso de confidencialidad y/o no concurrencia, una licencia de cesión de derechos de explotación sobre aquello creado, en beneficio del empresario. El TRLPI establece una presunción que regirá a falta de tal pacto, y que atribuye a la empresa determinados derechos sobre la obra

---

contrato de servicios de computación en la nube".

122 Sirva de ejemplo un servicio de plataforma *cloud* (PaaS), que permitiría a un usuario ejecutar en la nube todos los pasos de desarrollo, creación y prueba de una aplicación de gestión de recursos humanos para empresas turísticas o de un nuevo videojuego o aplicación móvil, o de un software como servicio (SaaS) que permita al cliente crear y compartir entre usuarios textos e imágenes.

123 Art. 5 del TRLPI: "1. Se considera autor a la persona natural que crea alguna obra literaria, artística o científica. 2.- No obstante de la protección que esta Ley concede al autor se podrán beneficiar personas jurídicas en los casos expresamente previstos en ella".

124 Ver apartado sobre confidencialidad de los datos de usuario, en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

de manera directa en su artículo 51[125]. Este artículo concede una cesión de los derechos de explotación en exclusiva al empresario, aunque limitada a finalidades comprendidas dentro de la actividad habitual del empresario. Según el mismo artículo, el empleado, por su parte, conservará los derechos morales de esa obra, aunque no podrá explotarla mientras se mantenga vigente esta cesión[126]. Asimismo, si lo creado es un programa de ordenador, el mismo artículo 51 remite al artículo 97.4 del TRLPI, el cual establece que corresponderán al empresario el código fuente y el programa objeto[127].

Las bases de datos se protegen de forma especial en el TRLPI, a través de una regulación genérica, recogida en su art.12, y otra *sui generis,* recogida en su Título VIII[128]. Así, el fabricante[129] de una base de datos (en atención a la definición del artículo 12 ya mencionado) posee el derecho de "prohibir la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido de esta, evaluada cualitativa o cuantitativamente, siempre que la obtención, la verificación o la presentación de dicho contenido representen una inversión sustancial desde el punto de vista cuantitativo o cualitativo". Este derecho es transferible mediante licencia o cesión.

---

125 Art. 51 TRLPI: "1. La transmisión al empresario de los derechos de explotación de la obra creada en virtud de una relación laboral se regirá por lo pactado en el contrato, debiendo éste realizarse por escrito. 2. A falta de pacto escrito, se presumirá que los derechos de explotación han sido cedidos en exclusiva y con el alcance necesario para el ejercicio de la actividad habitual del empresario en el momento de la entrega de la obra realizada en virtud de dicha relación laboral. 3. En ningún caso podrá el empresario utilizar la obra o disponer de ella para un sentido o fines diferentes de los que se derivan de lo establecido en los dos apartados anteriores. 4. Las demás disposiciones de esta Ley serán, en lo pertinente, de aplicación a estas transmisiones, siempre que así se derive de la finalidad y objeto del contrato. 5. La titularidad de los derechos sobre un programa de ordenador creado por un trabajador asalariado en el ejercicio de sus funciones o siguiendo las instrucciones de su empresario se regirá por lo previsto en el apartado 4 del artículo 97 de esta Ley".

126 Recordemos que los derechos morales del autor son irrenunciables e inalienables de acuerdo con el art. 14 del TRLPI.

127 Art. 97.4 TRLPI: "Cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador así creado, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario".

128 Al respecto, nos remitimos a VIVAS TESÓN, Inmaculada, "La doble protección jurídica de las bases de datos: derecho de autor y derecho sui géneris del fabricante", *Cuestiones de actualidad en el ámbito de la propiedad intelectual* (Coord. Inmaculada Vivas), 1ª edición, Madrid, 2015, págs. 145 a 173.

129 Según PARRA GRECO, "Se considerará fabricante a aquella persona natural o jurídica que tome la iniciativa y asuma el riesgo de la inversión sustancial orientada a la obtención, verificación y presentación del contenido de una base de datos". PARRA GRECO, Rosa, "Protección jurídica de las bases de datos", *Saberes: Revista de estudios jurídicos, económicos y sociales, Universidad Alfonso X El Sabio,* núm. 1, 2003, págs. 15 a 22.

4.3.2.- Creaciones desarrolladas fuera de una relación laboral

Como hemos mencionado, la titularidad y los derechos de explotación de una obra creada fuera del ámbito laboral pertenecen inicialmente a su creador (art. 5 LPI), quién podrá transmitir el ejercicio de los derechos de explotación (arts. 42 y 43 de la LPI) pero no los derechos morales (art. 14 LPI).

Existen ciertos servicios de computación remota específicos para que el suscriptor desarrolle su propio software, como los servicios *cloud* de plataforma. Sin embargo, no suele recogerse contractualmente el régimen jurídico o los derechos sobre las aplicaciones que el cliente desarrolla o despliega dentro de entornos en la nube. Así, el cliente puede reclamar sus derechos como creador en base al artículo 5 del TRLPI. Aunque en ocasiones no resulte sencillo delimitar la aplicación desarrollada por el usuario y las herramientas de la plataforma suministradas por el proveedor, en muchos casos puede entenderse que la tarea intelectual ha sido desarrollada exclusivamente por el cliente, mientras que el servicio *cloud* ha servido únicamente de manera instrumental, con lo cual el proveedor, a nuestro parecer, quedaría fuera de cualquier titularidad de los derechos de explotación de obras creadas gracias al uso de herramientas *cloud.* Si, a través de las condiciones generales de uso del servicio, se ha producido pactado alguna cesión de derechos sobre las obras creadas por el cliente mediante el uso del servicio en favor del proveedor *cloud*, esta cláusula sería susceptible de ser considerada abusiva. Todo lo anterior se entiende sin perjuicio de los derechos de propiedad intelectual e industrial referentes al propio servicio *cloud* suscrito por el cliente, y que puedan haber servido de base para su creación.

La regulación de los derechos sobre los programas informáticos está comprendida en los genéricos derechos morales del art. 14 del TRLPI, ya mencionados, y en los arts. 95 a 103 del mismo texto, específicos para programas de ordenador y su explotación, y es similar a la protección concedida a las obras literarias (como afirma el motivo 6 de la Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009 sobre la protección jurídica de programas de ordenador[130]). La protección abarca tanto el programa de ordenador ("se

130 Motivo Sexto de la Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009 sobre la protección jurídica de programas de ordenador: "En consecuencia, el marco

entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación", art. 96.1 TRLPI) como su código fuente, su documentación preparatoria y técnica, sus manuales de uso y sus sucesivas versiones o programas derivados, e independientemente de su funcionalidad. El programa informático debe ser original, y no bastarán meras mejoras en la calidad o estética para considerarlo como tal (según el motivo 8 de la Directiva 2009/24/CE).

Aunque la Ley de Patentes, en su art. 4.4.c[131], no permite patentar los programas de ordenador, por considerar que carecen del carácter de invención de aplicación industrial (es decir, no solucionan ningún problema técnico), sí pueden formar parte integrante de un conjunto considerado como invención patentable, formando parte del objeto sobre el cual recae la patente (art. 4.5 de la misma Ley[132])[133]. En este caso, la protección de los derechos de autor de los programas de ordenador es compatible con la protección brindada por la legislación de propiedad industrial (art. 96.3 TRLPI), siempre y cuando se cumpla con los requisitos de patentabilidad de las invenciones del art. 4.1 de la Ley de Patentes[134] (que sea una invención nueva, que implique actividad inventiva y que sean susceptibles de aplicación industrial).

Cuando lo desarrollado por el cliente *cloud* a través de herramientas en la

---

jurídico comunitario sobre protección de programas de ordenador puede, en primer término, limitarse a establecer que los Estados miembros deban conceder a dichos programas una protección con arreglo a la legislación sobre derechos de autor como obras literarias. Debe establecerse el sujeto y el objeto de la protección, los derechos exclusivos a los que pueden acogerse los sujetos de la protección para autorizar o prohibir determinados actos y la duración de dicha protección".

131 Art. 4.4.c) de la Ley 24/2015, de 24 de julio, de Patentes: "No se considerarán invenciones en el sentido de los apartados anteriores, en particular: (...) c) Los planes, reglas y métodos para el ejercicio de actividades intelectuales, para juegos o para actividades económico-comerciales, así como los programas de ordenadores".

132 Art. 4.5 de la Ley de Patentes. "Lo dispuesto en el apartado anterior excluye la patentabilidad de las invenciones mencionadas en el mismo solamente en la medida en que el objeto para el que la patente se solicita comprenda una de ellas".

133 BERCOVITZ RODRÍGUEZ-CANO, Alberto; "Sobre la patentabilidad de las invenciones referentes a programas de ordenador", *Novática, Revista de la Asociación de Técnicos de Informática,* núm. 163, 2003, págs 17- 20.

134 Art. 4.1 de la Ley de Patentes. "Son patentables las invenciones nuevas, que impliquen actividad inventiva y sean susceptibles de aplicación industrial, aun cuando tengan por objeto un producto que esté compuesto o que contenga materia biológica, o un procedimiento mediante el cual se produzca, transforme o utilice materia biológica".

nube es una base de datos, hemos mencionado anteriormente que nos encontramos ante una doble protección por parte del TRLPI. En primer lugar, la protección brindada por su art. 12[135], en la que no protege los contenidos accesibles gracias a la base de datos, sino su estructura original, es decir, su modo de selección u ordenación. En segundo lugar, es en su art. 133 donde radica la llamada protección *sui generis,* que no solo protege estrictamente los contenidos, sino la inversión sustancial realizada por el creador para llevar a cabo la búsqueda y recopilación de los datos ya existentes y que conforman los contenidos de la base de datos[136]. En relación a los usos legítimos, se le permite al usuario extraer o reutilizar sus contenidos en los casos mencionados en los arts. 134 y 135 del TRLPI[137]. Del mismo

135 Art. 12 TRLPI: "También son objeto de propiedad intelectual, en los términos del Libro I de la presente Ley, las colecciones de obras ajenas, de datos o de otros elementos independientes como las antologías y las bases de datos que por la selección o disposición de sus contenidos constituyan creaciones intelectuales, sin perjuicio, en su caso, de los derechos que pudieran subsistir sobre dichos contenidos. 2. La protección reconocida en el presente artículo a estas colecciones se refiere únicamente a su estructura en cuanto forma de expresión de la selección o disposición de sus contenidos, no siendo extensiva a éstos. A efectos de la presente Ley, y sin perjuicio de lo dispuesto en el apartado anterior, se consideran bases de datos las colecciones de obras, de datos, o de otros elementos independientes dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma. 3. La protección reconocida a las bases de datos en virtud del presente artículo no se aplicará a los programas de ordenador utilizados en la fabricación o en el funcionamiento de bases de datos accesibles por medios electrónicos".

136 Según PARRA GRECO, "El derecho *sui generis* protegerá la inversión sustancial, evaluada de forma cualitativa o cuantitativa, que realice el fabricante de la base de datos, ya sea de medios financieros, empleo de tiempo, esfuerzo u otros de similar naturaleza, para la obtención, verificación o presentación de su contenido. Es, por tanto, un derecho claramente diferenciado del derecho de autor, que protegerá la forma de estructura del contenido de una base de datos, y no el propio contenido". PARRA GRECO, Rosa, "Protección jurídica de las bases de datos", *Saberes: Revista de estudios jurídicos, económicos y sociales, Universidad Alfonso X El Sabio,* núm. 1, 2003, pág. 15 a 22.

137 Art. 134 TRLPI. "El fabricante de una base de datos, sea cual fuere la forma en que haya sido puesta a disposición del público, no podrá impedir al usuario legítimo de dicha base extraer y/o reutilizar partes no sustanciales de su contenido, evaluadas de forma cualitativa o cuantitativa, con independencia del fin a que se destine. En los supuestos en que el usuario legítimo esté autorizado a extraer y/o reutilizar sólo parte de la base de datos, lo dispuesto en el párrafo anterior se aplicará únicamente a dicha parte. 2. El usuario legítimo de una base de datos, sea cual fuere la forma en que haya sido puesta a disposición del público, no podrá efectuar los siguientes actos: a) Los que sean contrarios a una explotación normal de dicha base o lesionen injustificadamente los intereses legítimos del fabricante de la base. b) Los que perjudiquen al titular de un derecho de autor o de uno cualquiera de los derechos reconocidos en los Títulos I a VI del Libro II de la presente Ley que afecten a obras o prestaciones contenidas en dicha base. 3. Cualquier pacto en contrario a lo establecido en esta disposición será nulo de pleno derecho". Art. 135 TRLPI: "El usuario legítimo de una base de datos, sea cual fuere la forma en que ésta haya sido puesta a disposición del público, podrá, sin autorización del fabricante de la base, extraer y/o reutilizar una parte sustancial del contenido de la misma, en los siguientes casos: a) Cuando se trate de una extracción para fines privados del contenido de una base de datos no electrónica. b) Cuando se trate de una extracción con fines ilustrativos de enseñanza o de investigación científica en la medida justificada por el objetivo no comercial que se persiga y siempre que se indique la fuente. c) Cuando se trate de una extracción y/o reutilización para fines de seguridad pública o a

modo, el usuario también se verá privado de realizar aquellos actos que lesionen intereses legítimos del fabricante de dicha base de datos o de terceros titulares de derechos de autor de obras contenidas en la base de datos.

Esta protección jurídica *sui generis* de las bases de datos que acabamos de exponer es el resultado de la transposición de la Directiva 96/9/CE, y es inexistente en países fuera de la Unión Europea, como los Estados Unidos, cuyo *copyright* no ampara las inversiones realizadas por los recolectores de datos[138].

Si el usuario ofrece al proveedor sus ideas en cuanto a recomendaciones, sugerencias y mejoras sobre el servicio, el proveedor suele negar al usuario cualquier tipo de derecho o remuneración sobre ellas, tal y como puede reflejarse en muchas condiciones generales de servicios *cloud*[139]. Aunque en principio estas ideas o comentarios no son susceptibles de considerarse "obra" de acuerdo con el amparo ofrecido por el art. 10 de la LPI, con esta cláusula se establece la renuncia por parte del usuario de cualquier tipo de beneficio que pudiera derivarse de su idea o sugerencia[140].

---

efectos de un procedimiento administrativo o judicial. 2. Las disposiciones del apartado anterior no podrán interpretarse de manera tal que permita su aplicación de forma que cause un perjuicio injustificado a los intereses legítimos del titular del derecho o que vaya en detrimento de la explotación normal del objeto protegido".

138 En la decisión de la *US Supreme Court* sobre el caso "Feist Publications Inc *vs.* Rural Telephone Service Company Inc", donde la primera copió listados telefónicos de la segunda para incluirlos en los suyos después de que aquella le hubiese denegado su autorización para hacerlo, la Corte determinó que la información del directorio telefónico no era susceptible de cobijarse bajo la protección del *copyright*, puesto que carecía de originalidad, y que esta únicamente podría predicarse en el orden o el estilo de su presentación. Además, aseveró que la intención del *copyright* no era la de recompensar el esfuerzo recolector de los datos, y consideró irrelevante los dispendios monetarios y de tiempo. Por tanto, no existía infracción alguna bajo la legislación sobre *copyright.*

139 "Agradecemos los comentarios, pero ten en cuenta que podríamos usar cualquier comentario o sugerencia sin que ello implique ninguna obligación hacia ti por nuestra parte". Condiciones generales del software como servicio (SaaS) de almacenamiento Dropbox [en línea]. Disponible en: <https://www.dropbox.com/es_ES/privacy#terms>. [Fecha de consulta:8 de mayo de 2017].

140 Art. 10 TRLPI: "Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, comprendiéndose entre ellas: a) Los libros, folletos, impresos, epistolarios, escritos, discursos y alocuciones, conferencias, informes forenses, explicaciones de cátedra y cualesquiera otras obras de la misma naturaleza. b) Las composiciones musicales, con o sin letra. c) Las obras dramáticas y dramático-musicales, las coreografías, las pantomimas y, en general, las obras teatrales. d) Las obras cinematográficas y cualesquiera otras obras audiovisuales. e) Las esculturas y las obras de pintura, dibujo, grabado, litografía y las historietas gráficas, tebeos o cómics, así como sus ensayos o bocetos y las demás obras plásticas, sean o no

4.4.- Obras de autoría plural en la nube

En el mercado están surgiendo softwares como servicio y webs 2.0 que permiten crear obras a partir de las aportaciones de múltiples usuarios y de las herramientas software que el proveedor *cloud* pone a su disposición[141]. El fenómeno *Bring your own device*[142] parece extenderse a ámbitos que exceden la propia empresa, y entra en el ámbito de los usos mixtos privados y profesionales, permitiendo desarrollar en ambos ámbitos la creación de contenidos en cualquiera de sus expresiones artísticas, científicas o culturales, en ocasiones a través de mecanismos colaborativos.

En nuestra opinión, en este caso se trata de obras en colaboración, porque son resultado de las aportaciones que múltiples personas realizan gracias a la aplicación suministrada por el proveedor *cloud*. La regulación de las obras en colaboración en el TRLPI aparece en su artículo 7[143]. Sin embargo, no descartamos que, dependiendo de

---

aplicadas. f) Los proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería. g) Los gráficos, mapas y diseños relativos a la topografía, la geografía y, en general, a la ciencia. h) Las obras fotográficas y las expresadas por procedimiento análogo a la fotografía. i) Los programas de ordenador".

141 REED, Chris; Cunningham, Alan; "Ownership of information in Clouds", *Cloud Computing Law* (Coord. Christopher Millard), 1 edición, Oxford, 2013, pág 159. Un ejemplo de creación colaborativa es el periodismo participativo. La red social Cowbird permite contar historias de manera personal, y pretende formar una biblioteca pública de historias que reflejen la experiencia humana. Su comunidad exige, para ingresar como usuario, la aceptación de una licencia muy generosa sobre los contenidos publicados por los usuarios: "We do not claim ownership of the content that you submit for inclusion on Cowbird. However, with respect to content that you submit for inclusion on publicly accessible areas of the Cowbird services, you grant the company the following transferable, perpetual, irrevocable, sub-licensable, worldwide, royalty-free and non-exclusive license(s) to use, distribute, reproduce, modify, adapt, publicly perform and publicly display and exploit such content on and/or in connection with Cowbird (including distributing and featuring your content through messages such as a "Cowbird Daily Story" and in promotional and marketing activities and materials related to Cowbird). When these terms are terminated, we will make commercially reasonable efforts to remove and to respond to your requests to remove your content from Cowbird, but you acknowledge that we might retain copies of your content and other information provided to us as a part of our standard archive practices". Términos de la red social Cowbird [en línea]. Disponible en: <http://cowbird.com/terms/>. [Fecha de consulta: 8 de mayo de 2017].

142 *Bring your own device o* "trae tu propio dispositivo". Política empresarial que incentiva a sus empleados a acceder a información digital y a aplicaciones informáticas de la empresa a través de su propio dispositivo portátil (smartphone, tableta, ordenador portátil, etc.) También se aplica en el sector educativo. (Definición propia).

143 Art. 7 TRLPI. Obra en colaboración. "1. Los derechos sobre una obra que sea resultado unitario de la colaboración de varios autores corresponden a todos ellos. 2. Para divulgar y modificar la obra se requiere el consentimiento de todos los coautores. En defecto de acuerdo, el Juez resolverá. Una vez divulgada la obra, ningún coautor puede rehusar injustificadamente su consentimiento para su explotación en la forma en que

la concreta configuración del servicio, los resultados puedan considerarse obras colectivas de acuerdo con el artículo 8[144] u obras compuestas según el artículo 9 del mismo texto[145].

En cualquier caso, estos artículos deberán integrarse con lo establecido en el contrato, al cual deberán estar especialmente atentos consumidores y pequeños empresarios usuarios de estos servicios, ya que en las condiciones generales podrían encontrarse licencias de derechos o cesiones de titularidad en cuanto a obras de potencial valor comercial susceptibles de ser objeto de propiedad intelectual o industrial. Igualmente, puede ser relevante lo dispuesto por otra normativa de aplicación, como la normativa laboral y la protección al consumidor[146].

El resultado de estas creaciones puede ser una obra unitaria[147], o, por el contrario, varias obras derivadas[148]. Incluso puede dar lugar a una invención o diseño patentables o con potencial valor comercial. La divulgación y explotación de estas

---

se divulgó. 3. A reserva de lo pactado entre los coautores de la obra en colaboración, éstos podrán explotar separadamente sus aportaciones, salvo que causen perjuicio a la explotación común. 4. Los derechos de propiedad intelectual sobre una obra en colaboración corresponden a todos los autores en la proporción que ellos determinen. En lo no previsto en esta Ley, se aplicarán a estas obras las reglas establecidas en el Código Civil para la comunidad de bienes".

144 Art. 8 TRLPI. Obra colectiva. "Se considera obra colectiva la creada por la iniciativa y bajo la coordinación de una persona natural o jurídica que la edita y divulga bajo su nombre y está constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual haya sido concebida sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra realizada". Otra cuestión que plantean estas obras colectivas afectan a cuestiones de Derecho Internacional, especialmente en cuanto al tema de la jurisdicción y legislación aplicable: si los autores pertenecen a distintas nacionalidades, cosa muy probable si hablamos de aplicaciones accesibles a través de Internet, ¿qué ley sobre propiedad intelectual se aplicaría a estas obras colectivas: la del creador (o creadores) de la aportación principal o la determinada por el contrato suscrito con el proveedor? ¿Qué tribunales serían los competentes en caso de disputa?

145 Art. 9 TRLPI. Obras compuestas. "Se considerará obra compuesta la obra nueva que incorpore una obra preexistente sin la colaboración del autor de esta última, sin perjuicio de los derechos que a éste correspondan y de su necesaria autorización".

146 No nos detendremos, por razones de extensión y temática, en la resolución de estas cuestiones. Únicamente pretendemos dejar apuntada parte de la problemática existente en relación a la propiedad intelectual y la creación de obras en colaboración, como potencial funcionalidad disponible a través de computación remota.

147 Obra unitaria: los contenidos que resultan de la creación forman parte integrante de una única obra. (Definición propia).

148 Obra derivada. Los contenidos que resultan de la creación son fruto de la transformación, modificación o adaptación de una o varias obras preexistentes, las cuales a su vez pueden ser objeto de derechos de autor, y presentan alguna novedad respecto de la obra original. (Definición propia).

obras tradicionalmente necesita del consentimiento de todos sus autores, aunque si existe pacto, la explotación podrá realizarse de forma separada (art. 7.2 y 7.3 TRLPI).

Pero los entornos en la nube y las redes sociales propician la aparición de nuevos actores con intereses legítimos, con lo cual aparecen nuevas cuestiones: ¿se necesita consentimiento del proveedor para explotar la obra, puesto que como profesional ha facilitado el medio y ha posibilitado la creación? ¿Tiene derecho el proveedor a participar en los beneficios derivados de la explotación?[149] La respuesta a estas incógnitas debería quedar plasmada de antemano en la licencia previa suscrita al ingresar en el servicio que permita la creación colectiva de obras. Pero, ¿y si no existe tal acuerdo? Por nuestra parte, consideramos que debería atenderse al tipo de servicio (si se ha diseñado específicamente para la creación de obras o si su uso es meramente instrumental), a su gratuidad u onerosidad (a mayor onerosidad, menos derechos debería obtener el proveedor sobre la obra, puesto que ya recibe una contraprestación económica) y a la relevancia de la aportación del proveedor en la consecución de la obra (por ejemplo, si se hubiera podido obtener a partir de otros medios que no fuesen su plataforma).

Por otro lado, ¿tiene cualquier colaborador, por mínima que sea su aportación, derecho a manifestarse o a oponerse a la explotación? Parece lógico que se exija una aportación significativa para considerar a su autor como titular de algún derecho sobre la obra unitaria. Pero a veces resulta complicado determinar la importancia de las aportaciones cuando estas tienen lugar en línea o en tiempo real. Además, no siempre resultará factible identificar a los autores, puesto que la Red les permite mantener su anonimato si así lo desean, o que la obra sea fruto de aportaciones incontables o masivas[150].

Muchos de estos problemas pueden solucionarse con una adecuada redacción de los términos de uso del servicio *cloud* o de la red social en cuestión. No obstante, el usuario debe vigilar las licencias que concede sobre sus contenidos, y ser consciente de la imposibilidad de revocar ciertas licencias ya otorgadas. Asimismo, quizás sería conveniente idear otros modelos de titularidad colectiva, más equilibrados y específicos, adecuados a la nueva realidad facilitada por aplicaciones

149 REED, Chris; CUNNINGHAM, Alan, *op. cit.*, pág. 159.
150 REED, Chris; CUNNINGHAM, Alan, *op. cit.*, pág. 159.

descargables, webs 2.0 y softwares como servicio, que permitieran una gestión óptima de la explotación y que, en su caso, pudiese revertir en beneficios para quienes han realizado aportaciones o inversiones significativas.

4.5.- Herramientas que el proveedor pone a disposición del cliente

Una vez examinado el tratamiento contractual de los datos procesados en la nube por el cliente o usuario, otra de las previsiones habituales del contrato en relación a la propiedad intelectual y al uso de la información que fluye en la relación jurídica es la protección los contenidos que se proporcionan al cliente para una provechosa utilización del servicio, en otras palabras, los contenidos que atañen a las aplicaciones y funciones facilitadas por el proveedor.

Como hemos observado, la regulación sobre la propiedad intelectual de los programas de ordenador en España aparece recogida en el TRLPI, en concreto, en sus artículos 10.1, 95 a 104 y 114. También hemos visto que no es susceptible de patentarse, a no ser que forme parte integrante de una invención (art. 4.4.c de la Ley de Patentes)[151].

La normativa española permite al usuario legítimo, excepto pacto contrario, reproducir, transformar el programa o corregir errores bajo la condición de que sea necesario para la finalidad del programa (art. 100.4 TRLPI[152]). Sin embargo, para otras finalidades distintas será necesaria la autorización por el titular de los derechos de explotación del programa informático[153]. Igualmente será necesaria autorización del titular para la elaboración de sus sucesivas versiones y actualizaciones, cuyos derechos pertenecerán inicialmente a quienes las realice (arts. 11, 21 y 96.3 LPI[154]).

---

151 Además de lo anterior, debemos tener en cuenta la normativa que resulte aplicable al contrato y la norma nacional concreta bajo la cual ampare sus derechos el titular de los derechos de autor. Como sabemos, la contratación (y subcontratación) de servicios de computación en la *nube* es compleja, y suele integrar a actores (y normativas) de múltiples nacionalidades.

152 Art. 100.1 TRLPI. "No necesitarán autorización del titular, salvo disposición contractual en contrario, la reproducción o transformación de un programa de ordenador incluida la corrección de errores, cuando dichos actos sean necesarios para la utilización del mismo por parte del usuario legítimo, con arreglo a su finalidad propuesta".

153 Ver apartado "Contenidos titularidad de un tercero migrados a la nube por un usuario. El caso especial del software y las bases de datos", en este mismo capítulo.

154 Art. 96.3 TRLPI. "La protección prevista en la presente Ley se aplicará a cualquier forma de expresión de un programa de ordenador. Asimismo, esta protección se extiende a cualesquiera versiones sucesivas del programa así como a los programas derivados, salvo aquellas creadas con el fin de ocasionar efectos nocivos a

En la práctica contractual de los servicios en la *nube*, como hemos comprobado, suele dejarse claro que tanto las partes como los terceros conservan sus derechos de propiedad intelectual sobre los datos y sobre las herramientas que permiten la prestación del servicio.

Mediante la distribución de responsabilidades en el contrato de adhesión o a través de las políticas de uso adecuado (PUA), se advierte al suscriptor de su obligación de respetar los derechos de propiedad intelectual e industrial que correspondan al proveedor o a alguno de sus licenciantes. Consecuentemente, deberá responder por cualesquiera usos infractores de tales derechos que pueda ocasionar su actividad o la actividad que, en su caso, lleven a cabo los usuarios finales beneficiarios del servicio contratado por el cliente.

A menudo llama la atención el contraste entre los términos utilizados en la licencia de uso otorgada al suscriptor sobre los contenidos y herramientas que el proveedor pone a su disposición (que suele ser bastante clara en sus términos y restringida específicamente a la prestación del servicio *cloud),* y las licencias de uso de los contenidos facilitados por el usuario, que hemos examinado en apartados anteriores (las cuales, como hemos visto, son mucho más amplias y utilizan términos jurídicos imprecisos)[155].

---

un sistema informático. Cuando los programas de ordenador formen parte de una patente o un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial".

155 A continuación, veamos un ejemplo de licencia sobre programas informáticos puestos a disposición del cliente de servicios de Google, lo cual incluye sus servicios *cloud*: "Google te concede una licencia personal mundial, libre de royalties, intransmisible y no exclusiva para usar el software que se te proporcione como parte de los servicios. El único propósito de esta licencia es permitirte usar los servicios que ofrece Google y beneficiarte de ellos, según lo estipulado en estas condiciones. No podrás copiar, modificar, distribuir, vender ni prestar ninguna parte de nuestros servicios ni del software incluido ni podrás aplicar técnicas de ingeniería inversa ni intentar extraer el código fuente de dicho software, salvo si la legislación prohíbe dichas restricciones o si tienes consentimiento de Google por escrito". Hemos observado que la licencia que Google concede a sus usuarios es bastante más limitada que su recíproca obtenida del usuario a su favor como proveedor: "Al subir, almacenar o recibir contenido o al enviarlo a nuestros Servicios o a través de ellos, concedes a Google (y a sus colaboradores) una licencia mundial para usar, alojar, almacenar, reproducir, modificar, crear obras derivadas (por ejemplo, las que resulten de la traducción, la adaptación u otros cambios que realicemos para que tu contenido se adapte mejor a nuestros Servicios), comunicar, publicar, ejecutar o mostrar públicamente y distribuir dicho contenido. Google usará los derechos que le confiere esta licencia únicamente con el fin de proporcionar, promocionar y mejorar los Servicios y de desarrollar servicios nuevos. Esta licencia seguirá vigente incluso cuando dejes de usar nuestros Servicios (...)". Condiciones de servicio de Google. <https://www.google.es/intl/es/policies/terms/regional.html>. [Fecha de consulta: 8 de mayo de

También son frecuentes, en las PUA o en otros apartados del contrato, las prohibiciones de actuaciones de ingeniería inversa o de extracción del código fuente, las cuales podrían atentar contra los derechos de propiedad intelectual e industrial del proveedor o de terceros.

Además, el proveedor no solo suele establecer la revocabilidad de la licencia concedida al usuario[156], sino que, como hemos visto, es habitual que se reserve el derecho a la libre suspensión de la prestación del servicio, con lo cual cualquier usuario, presunto infractor de derechos de propiedad intelectual a ojos del proveedor, puede verse privado del suministro o ver cancelada su cuenta, en ocasiones sin aviso previo[157].

Finalmente, ante casos de infracción de derechos de propiedad intelectual, se ponen a disposición de los usuarios mecanismos de denuncia ante el proveedor, que pueden ser específicos para este tipo de infracciones[158].

4.6.- Datos generados por el proveedor o por terceros a partir de la información de los usuarios

El proveedor puede generar información a partir de la actividad del usuario de su servicio *cloud* para diferentes propósitos empresariales, como mantenimiento,

---

2017].

156 Condiciones de uso de Dropbox [en línea]. "Mientras cumplas estas condiciones, te concederemos una licencia limitada, revocable, no exclusiva e intransferible para usar el software, con la finalidad exclusiva de acceder a los servicios. (...)". Disponible en: <https://www.dropbox.com/es_ES/privacy#terms> [Fecha de consulta: 8 de mayo de 2017].

157 Condiciones de uso de Dropbox [en línea]. "Respetamos la propiedad intelectual de los demás y te pedimos que hagas lo mismo. Responderemos a los avisos de presuntas infracciones de copyright si se realizan de forma acorde a la ley, y tales avisos deben notificarse de acuerdo con nuestra política de copyright. Nos reservamos el derecho de eliminar o inhabilitar el Contenido presuntamente infractor y de cancelar las cuentas de los infractores reincidentes". Disponibles en: <https://www.dropbox.com/es_ES/privacy#terms>. [Fecha de consulta: 8 de mayo de 2017].

158 Condiciones del Servicio de Facebook [en línea]. "Te proporcionamos las herramientas necesarias para ayudarte a proteger tus derechos de propiedad intelectual. Para obtener más información, visita nuestra página *Cómo informar de presuntas infracciones de los derechos de propiedad intelectual* [la cursiva es nuestra]". Disponible en: <https://www.facebook.com/legal/terms?locale=es_ES>. [Fecha de consulta: 8 de mayo de 2017].

seguridad, soporte técnico, cálculo de los recursos consumidos para proceder a su facturación, o aplicación de mejoras del servicio, entre otros[159]. Debido a su naturaleza, sobre estos datos dudosamente van a subsistir derechos de propiedad intelectual (al no ser categorizables como "obra" según el TRLPI) o la protección legal del secreto empresarial o *know-how*. En cambio, sí estarán sujetos al deber de confidencialidad[160], sobre todo cuando, en su recolección, el proveedor se haya comprometido a restringir su destino a finalidades de uso interno[161].

Si, por otra parte, el proveedor ha decidido recabar la autorización del usuario para potenciales usos más allá de su propia operativa, a través de la suscripción del contrato de adhesión, el usuario deberá estar atento a lo acordado contractualmente respecto del cumplimiento del deber de confidencialidad y a lo regulado por la legislación sobre privacidad, para prevenir que terceros no autorizados puedan acceder a información susceptible de mantenerse como reservada.

Siendo así las cosas, ¿qué sucede si el proveedor decide explotar o ceder a terceros la información derivada de las actividades del cliente? ¿Tiene el cliente alguna potestad de control sobre el uso de esta información? ¿Infringe su transferencia el deber de confidencialidad?

En este punto deberemos diferenciar entre los datos asociados a la identidad del usuario y aquellos que han sido objeto de un proceso de anonimización y no permiten identificar al usuario que los ha generado. En virtud de la normativa de protección de datos[162], los usos de datos personales que trascienden el tratamiento

159 Esta información, que se obtiene a través de herramientas de monitorización, metadatos, *cookies* o sistemas de análisis de *Big Data,* entre otros, suele aportar diferentes tipos de datos: la IP desde la cual se ha ingresado al servicio, usuarios que han accedido, tiempos de acceso, contenidos a los que se ha accedido y las operaciones que se han realizado sobre estos contenidos, con quién se han compartido, etc. Incluso pueden obtenerse datos sobre otros contactos almacenados en el dispositivo del usuario, su geolocalización, los datos de navegación, las aplicaciones que utiliza, etc.

160 Ver capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

161 REED, Cris; CUNNINGHAM, Alan, "Ownership of Information in Clouds", *Cloud Computing Law,* (coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 150.

162 Art. 11 LOPD: "Comunicación de datos. 1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. 2. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una

interno por parte del proveedor necesitan de autorización previa del titular. Así, si por alguna razón se revelan datos del perfil personal de un usuario cuando se examinan comportamientos colectivos, puede infringirse la legislación sobre protección de datos si previamente no se ha notificado al titular de los datos personales la existencia de un tratamiento de datos personales con fines distintos a los indicados (por ejemplo con fines publicitarios), o no se ha requerido la autorización que permita al proveedor la cesión a terceros de dichos datos. Si además, implica transferir datos a otros países, deberán cumplirse los requisitos adicionales para transferencias internacionales de datos de carácter personal que impone la normativa que en su caso le sea aplicable[163].

En el caso de que se trate de datos que no puedan considerarse datos personales, cabrá reclamar por infracción del deber de confidencialidad del proveedor si se ha filtrado esta información a terceros o si se ha ocultado al cliente la utilización de esta información para usos que escapen de la gestión interna del proveedor, como se deriva de las obligaciones de custodia de la información resultante de la propia naturaleza del contrato.

Sin embargo, actualmente se ha manifestado un aumento del tráfico de datos derivados de la actividad de los usuarios[164], que provienen de la gestión del

---

Ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. 3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar. 4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable. 5. Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley. 6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores".

163 Ver capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

164 Ver apartado "Clasificación de los datos alojados en la nube", en este mismo capítulo.

denominado *Big Data*[165] y de procesos de extracción de datos (también llamados minería de datos o *data mining)*[166]*.* El rastreo y la posterior explotación de la información sobre la actividad del cliente, no solo en la nube, sino en otros sitios web de comercio electrónico, suele realizarse conjuntamente con la de otros usuarios de la Red, a través de técnicas informáticas avanzadas, procesándolos, cruzándolos y analizándolos con otros datos en grandes bases de datos[167]. Su valor no radica en la información extractada aisladamente considerada, sino en los patrones derivados del análisis y de la aplicación de los algoritmos que pueden detectar un cambio en el comportamiento de la población internauta que advierta de oportunidades en distintas áreas.

Estos datos son muy valorados en el ámbito de publicidad y venta, porque permiten predecir tendencias y comportamientos que las empresas pueden aprovechar para transformar sus modelos de negocio, así como mejorar la experiencia del cliente, al recibir una suerte de publicidad personalizada de aquellos productos y servicios que, por lo revelado por estas tendencias, parecen ser de su interés y, por tanto, será más propenso a consumir. Estos análisis pueden revelar otras informaciones nuevas y potencialmente valiosa: la viabilidad de proyectos públicos o privados, la prospección de opiniones sobre temas actuales, el resultado de sondeos sobre ideologías políticas, la predicción de oportunidades de negocio, el cambio de tendencias del mercado, etc.

Dos problemas pueden plantearse en relación a esta información extractada a partir de datos de los clientes: en primer lugar, que sea posible reutilizar la información sin el consentimiento del usuario cuyos datos se han extractado, puesto que, aunque esté anonimizada, se genera a partir de sus actividades (privadas o profesionales) en la Red; en segundo lugar, que a través de procesos técnicos se pueda revertir la anonimización e identificar a la persona física que se esconde tras

165 *Big Data*. "Activos de información caracterizados por su alto volumen, velocidad y variedad, que demandan soluciones innovadoras y eficientes de procesado para la mejora del conocimiento y toma de decisiones en las organizaciones". BEYER Mark; LANEY, Douglas; "The importance of ´Big Data´: A definition" [en línea], 2012. Disponible en: <https://www.gartner.com/doc/2057415/importance-big-data-definition>. [Fecha de consulta: 8 de mayo de 2017].

166 *Data mining*. Proceso que unifica campos de conocimiento como la inteligencia artificial o la estadística para extraer patrones y anomalías a través del procesamiento de información a gran escala existente en la Red. (Definición propia).

167 REED, Cris; CUNNINGHAM, Alan, *op. cit.,* pág. 181.

los datos presuntamente aislados de cualquier identidad[168].

Respecto del primer problema, en cuanto a su explotación, deberá considerarse si, atendiendo a la naturaleza de los datos comprometidos, estos datos pueden quedar protegidos por la normativa de los secretos empresariales o, en su caso, de propiedad intelectual. Si el cliente ha autorizado en las condiciones generales la cesión de esta información a terceros, puede haber renunciado a la confidencialidad sobre estos datos[169]. Si están anonimizados, no pueden vincularse con una identidad individual, y por ello no pueden considerarse datos de carácter personal.

En cambio, el proveedor no tendrá impedimento para ceder los datos si previamente a la cesión, ha obtenido la autorización del cliente y ha cumplido con las medidas de seguridad, exigencias para transferencia internacional de datos, la información en relación al fichero, y demás obligaciones sobre privacidad que le sean aplicables.

Respecto del segundo problema, si la técnica informática permitiese revertir la anonimización de estos datos y se pudiera identificar la actividad del usuario individual que la ha generado, el proveedor encargado de su custodia deberá maximizar las medidas de seguridad, como parte de su deber de diligencia y de cumplimiento de la normativa sobre protección de datos, para impedir que se lleve a cabo tal conexión y/o revelación[170]. Este deber de custodia y la evitación de brechas de confidencialidad, como veremos en el correspondiente apartado, no es absoluto, sino que depende del estado de la técnica y de las medidas de seguridad que tienen lugar en el sector, puesto que es utópica la garantía de seguridad total en entornos digitales y en Red.

La exigencia de contraprestación por parte del usuario a la cesión de esta información no parece, a nuestro modo de ver, posible, ya que el valor de esta información radica en su combinación con la información aportada por otros

168 REED, Cris; CUNNINGHAM, Alan, *op. cit.,* pág.152.

169 Ver apartado "La confidencialidad de los datos del cliente y las solicitudes de acceso a terceros", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

170 Ver capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

internautas y usuarios de la Red y los servicios, ya que es en estos análisis de datos abstractos donde se revelan las tendencias que le aportan valor comercial. Excepto que pueda demostrarse que el proveedor o el tercero explotador de los datos está perjudicando al usuario u obteniendo considerables beneficios económicos que hubiera podido recibir el usuario de forma individual si hubiese gestionado esa información por su propia cuenta, no existirá, en nuestra opinión, posibilidad de reclamación económica.

Capítulo Quinto

PRIVACIDAD EN LA NUBE:

PRINCIPALES CUESTIONES SOBRE

PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1.- INTRODUCCIÓN

En capítulos anteriores hemos analizado los principales riesgos organizativos, técnicos y legales para pequeños empresarios suscriptores de servicios de computación en la nube, quienes generalmente comparten la misma preocupación sobre estos servicios: el cumplimiento normativo en materia de privacidad. En este capítulo, nuestro objetivo es abordar la problemática de la normativa en materia de protección de datos en los servicios de *Cloud Computing*, y más concretamente, en aquellos servicios suscritos por el pequeño empresario bajo la modalidad de implementación de nube pública[1].

La seguridad y la protección de datos se consideran factores competitivos diferenciales dentro del sector de la computación en la nube[2]. Así, muchos clientes elegirán su proveedor basándose en las garantías que ofrezca en cuanto a

1 Ver capítulo "Concepto y características técnicas de la computación en la nube".

2 ENISA, *Cloud Computing: Benefits, Risks and recommendations for information security* [en línea], 2012. Disponible en: <https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security>. [Fecha de consulta:9 de mayo de 2017].

confidencialidad e integridad de los datos migrados, y la fiabilidad de sus sistemas.

Del mismo modo, el cumplimiento de la legislación europea de protección de datos de carácter personal supone una de las principales preocupaciones cuando los pequeños empresarios deciden externalizar parte de su infraestructura informática a través de servicios *cloud*. Además, al tener que preocuparse por el coste de los servicios, a estos empresarios les será de gran utilidad una oferta extensa en el mercado que les garantice el respeto al marco legal, así como la existencia de servicios complementarios de asesoramiento en materia de privacidad. Igualmente, pueden serles de gran ayuda el apoyo y las recomendaciones de las autoridades reguladoras[3].

Pues bien, aunque la aplicación práctica de la normativa sobre protección de datos en el mundo físico y en los sistemas tradicionales de gestión está consolidada, su cumplimiento en el ámbito virtual presenta actualmente múltiples retos[4]. En especial, al combinar datos personales y servicios de computación en la nube, aparecen ciertas divergencias. Estas divergencias pueden ser conceptuales (como sucede con la categorización del proveedor *cloud* como mero encargado del fichero, cuando en la práctica actual resulta ser quien ostenta el mayor grado de control sobre los datos una vez que estos han sido migrados a la nube) o fácticas (como la entrada en juego de múltiples jurisdicciones con diferente concepción legal de la privacidad y, consecuentemente, con diferentes obligaciones y responsabilidades para cada una de las partes contractuales).

Por añadidura, la externalización de datos personales a través de su transferencia a proveedores *cloud* dificulta al empresario cliente, como responsable de tales datos, la efectiva comprobación y control de las prácticas de gestión de esos datos personales, llevadas a cabo por el proveedor y sus eventuales subproveedores. Dedicaremos este capítulo a algunos de estos problemas y a otras implicaciones jurídicas de la protección de datos en los contratos de servicios de computación en la nube. Asimismo, cabe decir que la diferente información facilitada por el proveedor *cloud* al suscriptor de los servicios que sea referente a la materia de protección de

3 GARCÍA SÁNCHEZ, Manuel, "Retos de la computación en la nube", *Derecho y Cloud Computing* (Coord. Ricard Martínez Martínez), 1ª edición, Navarra, 2012, pág. 49.

4 En el capítulo "Concepto y características técnicas de la computación en la nube", en este mismo trabajo, se relacionan los principales riesgos que presentan los entornos de computación en la nube. Sin embargo, en este capítulo nos centraremos en los riesgos que pueden afectar a la privacidad, recogidos como fundamentales por nuestra Constitución y que son regulados de manera especial por la normativa de protección de datos de carácter personal.

datos puede encontrarse distribuida u organizada en diferentes documentos o anexos contractuales, por ejemplo en acuerdos de nivel de servicio (como se verá en posteriores capítulos, a modo de objetivos de nivel de servicio), en políticas de privacidad o en el mismo clausulado contractual.

El Grupo de Trabajo del artículo 29 apunta, en su Dictamen 5/2012 sobre *Cloud Computing,* algunos riesgos de la implementación masiva de la computación en la nube en cuanto al cumplimiento de la normativa sobre privacidad: "la implantación a gran escala de servicios de computación en nube presenta una serie de riesgos, centrados en la falta de control sobre el uso de los datos de carácter personal"[5]. Otro factor de riesgo apuntado por mismo Dictamen es "la ausencia de información suficiente acerca de cómo, dónde y quién realizará el tratamiento de los datos". Este desconocimiento puede abocar a tratamientos de datos en jurisdicciones sin garantías legales equivalentes a las proporcionadas por el marco normativo europeo. Como consecuencia, "es posible que no puedan aplicar las medidas técnicas y organizativas necesarias para garantizar, por ejemplo, la disponibilidad y confidencialidad de los datos, de los que el cliente de los servicios en la nube continúa siendo jurídicamente responsable conforme a la legislación de la Unión Europea"[6].

Así la cosas, el Grupo de Trabajo recomienda a las organizaciones que deseen utilizar servicios *cloud* "un análisis exhaustivo y riguroso de los riesgos"[7]. La magnitud de estos riesgos variará dependiendo del modelo de nube (privada, pública o híbrida) y del tipo de servicio contratado (software como servicio, plataforma como servicio o infraestructura como servicio), así como de la sensibilidad de los datos que pretendan migrarse a la nube[8].

Si se producen brechas en las medidas de seguridad que garantizan la privacidad, las consecuencias para las empresas suscriptoras de servicios en la nube pueden ser económicamente importantes. Los costes internos y externos para

5 El Grupo de Trabajo del Artículo 29, del cual hablaremos más adelante, es un órgano independiente que integra a representantes de las autoridades nacionales de los Estados miembros de la Unión Europea (en nuestro caso, la Agencia Española de Protección de Datos) y tiene funciones consultivas. Su Dictamen 05/2012 sobre el *Cloud Computing* (WP 196) [en línea] está disponible en: <http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/julio/120701_NP_29_Cloud.pdf>. [Fecha de consulta: 9 de mayo de 2017].

6 Nota de prensa del Grupo de Trabajo del Art. 29, referente a su Opinión 05/2012 sobre el *Cloud Computing* (WP 196).

7 Nota de prensa del Grupo de Trabajo del Art. 29, referente a su Opinión 05/2012 sobre el *Cloud Computing* (WP 196).

8 Como hemos mencionado, nuestro trabajo se centrará en la modalidad de implementación pública y suscrita a través de contratos de adhesión por pequeños empresarios.

remediar eventuales brechas o minimizar sus consecuencias pueden tener múltiples causas: notificaciones a los afectados, indemnizaciones a terceros por incumplimiento legal o contractual, sanciones administrativas e incluso penales, o pérdida de ventaja competitiva y demás efectos de un impacto reputacional negativo, entre otros. Asimismo, en ocasiones existirán costes derivados de rehacer y reorganizar los datos personales y las consecuencias económicas para la empresa de que esos datos no estén disponibles en cierto momento, o que se encuentren desactualizados[9].

Por ello, los suscriptores (y en especial los pequeños empresarios sin oportunidades para negociar el contrato), atendiendo a la especial naturaleza de los servicios *cloud*, deben prestar atención a los derechos y obligaciones recogidos en los contratos, y en particular a las cláusulas relacionadas con los usos de los datos recogidos, las medidas de seguridad para protegerlos, la notificación de incidentes al cliente, las transferencias de datos, las subcontrataciones y sus garantías, el acceso a datos por parte de autoridades, y, por último, a la portabilidad y borrado de datos una vez extinguida la relación contractual. A estos efectos, puede ser de utilidad la guía publicada por la agencia europea ENISA (*European Network and Information Security Agency*), titulada *Cloud Security Guide for SMEs*[10], que facilita

9 MORALES, Juan Ramón, "Cloud computing: riesgos corporativos e implicaciones jurídicas" [en línea], *Actualidad Jurídica Aranzadi,* núm. 863. [Fecha de consulta: 18 de agosto de 2016]. Disponible en: <http://www.garrigues.com/es_ES/noticia/cloud-computing-riesgos-corporativos-e-implicaciones-juridicas>. En el mismo sentido, MARCHINI, Renzo; *Cloud Computing: a practical introduction to the legal issues,* 1ª edición, Londres, 2010, págs. 39-40.

10 La agencia de la Unión Europea ENISA publicó en abril de 2015 una guía de seguridad para las PYME que deseen implementar servicios en nube, que les sirva de ayuda para garantizar la seguridad de sus datos y evaluar los riesgos y oportunidades de los servicios en la nube. Esta guía destaca 11 riesgos de seguridad (entre ellos, cuestiones relacionadas con jurisdicciones extranjeras o potenciales conflictos legales o administrativos); 11 oportunidades de seguridad (elasticidad o reducción de costes para la PYME en seguridad física y lógica); y 12 preguntas específicas dirigidas a recabar la información relevante sobre seguridad del proveedor *cloud* escogido, con el fin de obtener un adecuado nivel de comprensión sobre el servicio contratado. También ha desarrollado una herramienta de seguridad en línea, para calcular y visualizar riesgos, oportunidades y personalizar la lista de preguntas sobre seguridad, para facilitar a las PYME la implementación de servicios en la nube y reducir su exposición a amenazas. Tanto la guía como la herramienta están disponibles en línea en la página web de la Agencia: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes> y <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/sme-guide-tool>, respectivamente. [Fecha de consulta: 9 de mayo de 2017]. Por último, cabe decir que la Agencia ENISA aparece regulada por los Reglamentos 460/2004 (ya derogado) y 526/2013; y que entre sus funciones se encuentra la asistencia a las instituciones europeas y a los Estados miembro en cuestiones técnicas que permitan

recomendaciones y buenas prácticas sobre seguridad de la información[11]. Por otra parte, el Grupo de Expertos en contratos de *Cloud Computing* (denominado *Cloud Select Industry Group* o C-SIG) de la Comisión Europea, en el marco de la *Cloud Computing Strategy*, está tramitando actualmente un código de conducta para proveedores de servicios *cloud* en materia de protección de datos, como se verá más adelante (*Data Protection Code of Conduct fod Cloud Service Providers*).

Una vez efectuadas las consideraciones anteriores, empezaremos este capítulo exponiendo el marco normativo europeo y español actual. A continuación, nos aproximaremos a los principales conceptos recogidos en la legislación y veremos cómo se produce su traslado al ámbito de los servicios de computación en la nube. Finalizaremos con el análisis de la problemática de las transferencias de datos y la regulación de la protección de datos de carácter personal entre proveedores y empresarios suscriptores de contratos de adhesión de servicios *cloud.*

2.- MARCO NORMATIVO EUROPEO Y ESPAÑOL DE LA PROTECCIÓN DE DATOS PERSONALES

La legislación europea en materia de protección de datos de carácter personal está orientada a proteger la privacidad de los ciudadanos europeos. En el momento de redacción de estas páginas, la norma europea reguladora de la protección de datos que es de aplicación es la Directiva 95/46/CE 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[12], aunque recientemente se ha

el desarrollo de legislación europea en los campos de seguridad de las redes de la información.

11 El Grupo de Trabajo IV de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), en su 55ª sesión, que tuvo lugar en fechas de 24 a 28 de abril de 2017 en Nueva York, recogió en la Nota de la Secretaría referente al trabajo sobre "Aspectos contractuales de la computación en la nube/ (A/CN.9/WG.4/WP.142) ciertas reticencias de los expertos en relación a la inclusión de cuestiones relacionadas con la privacidad en el texto orientativo que prepara la CNUDMI sobre la contratación internacional de computación en la nube: "No obstante, se dijo que convenía proceder con cautela para evitar tratar cuestiones como la protección de los datos, la privacidad y (...), que podrían no ser fáciles de armonizar y dar lugar a que se cuestionara si estaban comprendidas en el mandato de la Comisión". Disponible en el sitio web oficial de la CNUDMI: <http://www.uncitral.org/uncitral/es/commission/working_groups/4Electronic_Commerce.html>. [Fecha de consulta: 6 de junio de 2017].

12 Esta Directiva será aplicable, como establece en su art. 4, una vez transpuesta al derecho nacional: cuando el tratamiento tenga lugar por un responsable del tratamiento establecido en territorio de uno o más Estados miembro; cuando se deba aplicar, al responsable del tratamiento que no esté

aprobado el nuevo 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)[13]. Este Reglamento no será aplicable hasta el día 25 de mayo de 2018, fecha en la que substituirá definitivamente a la mencionada Directiva. Mientras tanto, los Estados miembro podrán realizar las adaptaciones necesarias a este nuevo marco[14].

---

establecido en territorio del Estado miembro, el derecho nacional en cumplimiento del Derecho internacional público; o cuando el responsable sin establecimiento en la Unión Europea recurra a medios para el tratamiento situados en un Estado miembro, excepto que tal uso se deba a motivos exclusivamente de tráfico. "Art. 4.1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable; b) el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público; c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea. 2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento".

13 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). Bruselas, 25.1.2012 COM (2012) 11 final. En adelante, también Reglamento europeo. No está de más puntualizar que esta nueva regulación comunitaria de la privacidad viene configurada como un reglamento, que es la norma comunitaria más vinculante. El artículo 288 del Tratado de Funcionamiento de la Unión Europea distingue entre los diferentes actos jurídicos que pueden adoptar las instituciones de la Unión Europea en el ejercicio de sus funciones: el reglamento, la directiva, las decisiones, las recomendaciones y los dictámenes. En concreto, dice del reglamento que "tendrá un alcance general. Será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro". La directiva europea, en cambio, "obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios". Este instrumento legal carece de la flexibilidad de la directiva, no tiene necesidad de ser transpuesto para producir sus efectos sobre las instituciones y los particulares de las naciones comunitarias y cualquier ciudadano europeo puede invocarlo ante los tribunales nacionales y demandar su cumplimiento. Se trata de una norma extensa, con 173 considerandos y 99 artículos agrupados en 11 capítulos.

14 En el artículo 99, el Reglamento establece: "El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea. 2. Será aplicable a partir del 25 de mayo de 2018. El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro". Publicado en el DOCE en fecha 4 de mayo de 2016, el Reglamento entró en vigor el 25 de mayo de 2016, aunque no resulta directamente aplicable a los países miembros hasta el 25 de mayo de 2018, pudiendo considerarse hasta entonces una suerte de *vacatio legis*. Durante este tiempo, los Estados miembro pueden adoptar nuevas normas que faciliten la aplicación del Reglamento, aunque no pueden ser contrarias al marco normativo vigente (excepto que, como el Reglamento, pospongan su aplicación hasta el momento en que sean derogadas las normas que

Hasta entonces, tanto la Directiva 95/46/CE como las normas nacionales que la transponen seguirán siendo aplicables. Debido a la inminente entrada en vigor del Reglamento General de Protección de Datos, en este trabajo realizaremos distintas referencias sobre sus diferentes disposiciones.

Un cambio importante es que el ámbito de aplicación territorial del nuevo Reglamento se ha ampliado para proporcionar garantías adicionales a los ciudadanos europeos que, por razón de transacciones en línea o monitorizaciones de comportamientos en la Red, veían como los tratamientos de sus datos se regían por normas con un nivel de protección de datos diferente (generalmente, menos proteccionista). Según su artículo 3, el Reglamento será aplicable cuando los datos personales de ciudadanos europeos sean tratados por un responsable o un encargado no establecido en la Unión con motivo de la oferta de bienes o servicios a los interesados (sin que sea relevante la remuneración por tal bien o servicio) o cuando estos responsables o encargados realicen seguimientos del comportamiento de los titulares de los datos personales si tal comportamiento tiene lugar en la Unión Europea[15].

Una de las principales novedades del Reglamento europeo es la aparición de

integran este marco) ni exceder de las competencias otorgadas por el propio Reglamento. También las organizaciones que traten datos personales pueden aprovechar este periodo para prepararse para los cambios que supondrá la plena aplicabilidad del Reglamento Europeo, e implementar las medidas previstas, siempre y cuando no contradigan la aún vigente Ley Orgánica de Protección de Datos. Así lo afirma la AEPD en la nota de prensa publicada en su sitio web. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "El Reglamento de Protección de Datos en 12 preguntas" [en línea], 2016. Disponible en: <https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php>. Fecha de consulta: 22 de agosto de 2016]. Junto a esta norma, se ha publicado la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

15 En el artículo 3 del Reglamento se determina su ámbito territorial: "El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión. 3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público".

nuevas figuras personales como el delegado de protección de datos (arts. 37 a 39 del Reglamento europeo), el representante en la Unión de responsables establecidos fuera de la Unión Europea (art. 27) o el Comité Europeo de Protección de Datos, que substituirá al Grupo de Trabajo del Artículo 29 (arts. 68 a 76 del Reglamento)[16].

Asimismo, el Reglamento también contiene nuevos derechos para los interesados, como la regulación de los derechos a limitar el tratamiento (art. 18), el derecho al olvido y a la supresión de datos (art. 17) y la introducción del derecho a la portabilidad (art. 20). También se regula el derecho a la oposición (art. 21), incluyendo el derecho a oponerse a la elaboración de perfiles susceptibles de producir efectos jurídicos (art. 22). Se mantienen el derecho de acceso al interesado (art. 15 del Reglamento) a los datos personales que le conciernen y el derecho a obtener información sobre el tratamiento que el responsable realiza de sus datos personales (fines, categorías de datos, destinatarios, plazos de conservación, elaboración de perfiles, garantías adecuadas ante transferencias internacionales, etc.), así como el derecho a rectificar esos datos (art. 16).

En cuanto a las obligaciones, cabe destacar como novedad la obligación de notificar las violaciones de datos personales, tanto del encargado al responsable, como del responsable a la autoridad de control (art. 33 del Reglamento) y, eventualmente, a los interesados que puedan ver sus derechos afectados (art. 34 del Reglamento).

Muchas de estas novedades del Reglamento europeo, en nuestra opinión, pueden considerarse buenas iniciativas y calificarse como reformas necesarias y

16 Si bien la figura del representante aparece definida en el artículo 4 del Reglamento como "persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento", el delegado de protección de datos no es objeto de definición, lo que lleva a pensar, más que en un descuido del legislador (puesto que sí aparecía definido en documentos preparatorios, como el Documento de Trabajo de los servicios de la Comisión relativo a la evaluación de impacto de su propuesta (SEC(2012) 72 final, de 25 de enero), en una omisión consciente y destinada a no restringir esta figura. Por otra parte, el apartado 5 del artículo 37 establece que el delegado "será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39", y según el apartado 6 del mismo artículo "el delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios". RECIO GAYO, Miguel; "El perfil jurídico del delegado de protección de datos" [en línea], 2016. Disponible en: <http://www.abogacia.es/2016/04/25/el-perfil-juridico-del-delegado-de-proteccion-de-datos/>. [Fecha de consulta: 9 de mayo de 2017].

útiles en cuanto a su aplicación en el ámbito de la computación en la nube[17].

Continuando con el marco normativo europeo, también son igualmente relevantes la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[18] y su posterior modificación realizada por la Directiva 2009/136/CE, también llamada Directiva de *cookies.* Estas Directivas se transpusieron al ordenamiento jurídico español a través de las reformas de la Ley General de Telecomunicaciones 32/2003, (derogada por la actual Ley 9/2014 de Telecomunicaciones), la Ley Orgánica de Protección de Datos de Carácter Personal y la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico[19].

Por otra parte, aunque no sean instrumentos legales estrictamente, debido a su influencia en el marco regulador, queremos hacer referencia al *Cloud Industry Group* (C-SIG), dedicado a establecer cláusulas estándar de contratos. Este grupo de trabajo se halla en el marco de la *European Cloud Computing Strategy* de la Comisión Europea, y ha dedicado algunas de sus actividades a estudiar específicos problemas que presenta la aplicación de la normativa comunitaria sobre protección

17 Existen otros cambios en esta extensa regulación que igualmente afectarán al tratamiento de datos que tenga lugar dentro de una relación contractual de computación en la nube, tanto si los servicios se suscriben por empresas (responsables del tratamiento de sus clientes) como por particulares (interesados titulares de datos de carácter personal). Nos referimos a los principios generales que deben regir el tratamiento (art. 5); aspectos relacionados con el consentimiento y sus condiciones para entenderlo como válido (arts. 7 y 8); el registro con la información de las actividades de tratamiento de datos (art. 30); o la regulación relacionada con las transferencias internacionales de datos (arts. 44 a 50), entre otros.

18 La transposición de esta Directiva supone obligaciones para los proveedores de servicios comerciales de comunicaciones electrónicas, entre las que destacan el secreto de las comunicaciones; la protección de sus servicios contra pérdidas, alteraciones accidentales, tratamientos o accesos no autorizados a datos de carácter personal; y la aplicación de políticas de seguridad, el consentimiento del usuario en caso de comunicaciones electrónicas y las notificaciones de brechas de seguridad a las autoridades nacionales y, en algunos casos, a los abonados afectados. Cuando dejen de ser necesarios para la comunicación o facturación, los datos relativos al tráfico deben borrarse o volverse anónimos. No obstante, los proveedores de servicios pueden tratar estos datos con fines comerciales durante el tiempo para el cual los usuarios hayan dado su consentimiento. Tal consentimiento podrá ser retirado por el interesado en cualquier momento.

19 Las principales reformas que acometió la transposición de esta Directiva son la captación del consentimiento expreso del usuario en cuanto al uso de las *cookies* y el ulterior tratamiento de los datos. Para más detalles sobre la aplicación de la normativa en el uso de *cookies*, es interesante la publicación realizada por la AEPD con título "Guía sobre el uso de las *cookies*". [en línea]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf>. [Fecha de consulta: 9 de mayo de 2017].

de datos de carácter personal en los entornos de computación en la nube[20]. Actualmente, está elaborando el *Data Protection Code of Conduct fod Cloud Service Providers,* un código de conducta en materia de privacidad que podrán suscribir voluntariamente aquellos proveedores de servicios *cloud* que lo deseen. Así, se pretende que este código de conducta contribuya a alcanzar una mayor transparencia y seguridad jurídica en las relaciones entre los adherentes al código de conducta y los suscriptores de sus servicios *cloud,* dado que puede servir de complemento a la legislación comunitaria en materia de privacidad y a su aplicación práctica en el marco de la contratación de estos servicios. El texto de este código de conducta se puso a disposición del Grupo de Trabajo del Artículo 29 para su análisis, y actualmente se halla en fase de revisión de las recomendaciones efectuadas por el Grupo de Trabajo del Artículo 29, con lo cual estamos a la espera de la publicación del texto definitivo[21].

Igualmente, otros acuerdos se están gestando entre EE. UU. y la Unión Europea que pueden resultar especialmente relevantes en materia de protección de datos y contratación de servicios de computación en la nube. Entre ellos, podemos destacar el *EU-USA Data Protection Umbrella Agreement*, firmado por los

20 Sirvan de ejemplo los *Discussion Papers* sobre transferencias de datos en la nube o sobre la responsabilidad por incumplimiento de las obligaciones en materia de protección de datos. Están disponibles en la página web oficial de la *Cloud Computing Strategy:* <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 9 de mayo de 2017]. Estas cuestiones serán tratadas en apartados posteriores de este mismo capítulo.

21 El Grupo de Trabajo del Artículo 29 manifiesta en su Opinión 2/2015 sobre el Código de Conducta sobre *Cloud Computing* del C-SIG, adoptada el 22 de septiembre de 2015, que no puede proceder a la aprobación formal del texto propuesto, y centra su atención en algunos aspectos que considera que deben mejorarse. En particular, la Opinión propone mejoras en cuanto a las consecuencias de la adherencia al código, a la distribución de responsabilidades asumidas por el proveedor *cloud* en su eventual papel de responsable, encargado o subencargado, a la transparencia en cuanto a la localización de los datos que se están procesando, al tratamiento de datos especialmente sensibles, al cumplimiento de las exigencias en materia de transferencias internacionales de datos y a los requisitos de acceso a datos personales por parte de autoridades, a las medidas de seguridad adoptadas y al nivel de detalle sobre su adopción, y a la necesidad de referirse a la portabilidad como un derecho del usuario, entre otras cuestiones. A pesar de lo anterior, el Grupo de Trabajo del Artículo 29 anima al C-SIG a continuar con el desarrollo del código de conducta y reconoce el valor que un código de estas características puede aportar a la industria de la computación en la nube y afirma que puede ser de gran ayuda a aquellos responsables del tratamiento (en el caso que nos ocupa, pequeños empresarios) que pretendan suscribir servicios *cloud*. Información sobre el Código de Conducta, su estado de tramitación y la Opinión del Grupo del Artículo 29 al respecto disponible en el sitio web de la Comisión Europea destinado a tal efecto: <https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers>. [Fecha de consulta: 6 de junio de 2017].

representantes de ambos territorios en fecha 2 de junio de 2016[22]. Según las informaciones oficiales, este acuerdo incrementará las garantías en materia de transferencias de datos entre autoridades competentes en materia de inteligencia y seguridad nacional, reforzando los derechos fundamentales y facilitando la cooperación entre las autoridades estadounidenses y comunitarias[23].

Por último, debemos tener en cuenta la relevancia, en materia de transferencia internacional de datos, de las Decisiones de la Comisión Europea, sobre países cuya normativa ofrece un nivel adecuado en materia de protección de datos y sobre cláusulas modelo[24].

Las autoridades de control nacionales (como la AEPD), por su parte, son competentes para adoptar otras garantías que permitan proteger los derechos de los titulares europeos de datos personales, como se verá en posteriores apartados. Más adelante haremos especial referencia también, por su importancia, al nuevo acuerdo,

22 Será aplicable el primer día del mes siguiente en que las partes se hayan comunicado mutuamente el fin de sus procedimientos internos de adaptación a este Acuerdo (art. 29 del Acuerdo). Para más información, ver Nota de prensa oficial de la Comisión Europea sobre el fin de las negociaciones del "*EU-US Data Protection Umbrella Agreeement*" [en línea]. Disponible en: <http://ec.europa.eu/justice/newsroom/data-protection/news/150908_en.htm>; nota de prensa sobre el contenido del Acuerdo [en línea], disponible en:<http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm>; nota de prensa de la firma del Acuerdo [en línea], disponible en:<http://ec.europa.eu/justice/newsroom/data-protection/news/160602_en.htm>, y texto del Acuerdo [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf>. [Fecha de consulta: 9 de mayo de 2017].

23 En los últimos años la Unión Europea ha estado trabajando en el Tratado de Libre Comercio entre la UE y EE. UU, que pretende eliminar las barreras arancelarias, burocráticas y legales que faciliten el comercio transatlántico, e impulsar la exportación de productos y servicios a PYME a ambos lados del Atlántico y la protección de la propiedad intelectual e industrial. En nuestra opinión sería posible que, en el marco de este acuerdo, se llegara a algún acercamiento de posiciones en cuanto a la protección de datos de consumidores europeos, e igualmente se acerquen posiciones en cuanto a la prestación de servicios a través de Internet (como es el caso de la computación en la nube) que tengan lugar entre empresas de ambos territorios. Sin embargo, parece que el reciente cambio político en la presidencia de EE. UU. ha frenado los avances en las negociaciones de este acuerdo bilateral. Para más información sobre el contenido de este Tratado y el estado de las negociaciones, podemos acudir a la página web de la Unión Europea. Disponible en: <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1249&serie=866&langId=es>. [Fecha de consulta: 9 de mayo de 2017].

24 En fecha 6 de octubre de 2015, en relación con el asunto C362/2014, (caso Maximilian Schrems) el Tribunal de Justicia de la Unión Europea ha declarado la nulidad de la Decisión 2000/520/UE sobre la adecuación 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. Dada su relevancia, profundizaremos en este tema en posteriores apartados de este capítulo.

denominado *Shield,* entre EE.UU y la Unión Europea, que substituye al anterior acuerdo *Safe Harbor*.

Por otra parte, como ya hemos expuesto, en virtud de la Directiva 95/46/CE se creó el *Art. 29 Working Party* o Grupo de Trabajo del Artículo 29, un órgano europeo de carácter independiente y con funciones consultivas, especializado en protección de datos[25]. Sus funciones principales son aclarar los conceptos y las obligaciones establecidas por la normativa europea, emitir dictámenes sobre el nivel de protección en la Unión y en terceros países, y formular recomendaciones sobre cuestiones relacionadas con la privacidad. Sin embargo, no determina los mecanismos técnicos que permiten cumplir con la legislación, puesto que para ello deberá acudirse a los diferentes ordenamientos nacionales. En las cuestiones que nos ocupan, resulta especialmente relevante el Dictamen 5/2012 sobre computación en nube[26].

En el ámbito de España, la transposición de la Directiva 95/46/CE tuvo lugar a través de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD), y se desarrolló mediante el Reglamento aprobado por Real Decreto 1720/2007, de 21 de diciembre (en adelante, RLOPD). El artículo 2.1 LOPD y el artículo 3.1 del RLOPD delimitan el ámbito territorial de aplicación de la normativa española en materia de protección de datos, vigente, como hemos comentado, hasta la fecha en que sea aplicable el Reglamento Europeo de Protección de Datos[27].

---

25 Sitio web oficial del Grupo de Trabajo del Artículo 29. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>. [Fecha de consulta: 9 de mayo de 2017]

26 GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 5/2012 sobre computación en nube* (WP 196) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf>. [Fecha de consulta: 9 de mayo de 2017]. La AEPD ha referenciado las consideraciones del Dictamen 5/2010 sobre *Cloud Computing* del Grupo de Trabajo del Artículo 29 en posteriores respuestas a consultas sobre la si algunas cláusulas sobre contratación de servicios de computación en la nube por parte de pequeños empresarios. A modo de ejemplo, el informe 0464/2012 de la Agencia de Protección de Datos, en respuesta a una consulta efectuada por un centro médico sobre si las cláusulas contractuales aportadas por un proveedor de servicios *cloud* se ajustaban a la LOPD [en línea]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2012-0464_Contrataci-oo-n-de-servicio-de-cloud-computing-por-cl-ii-nica-m-ee-dica.pdf>. [Fecha de consulta: 12 de mayo de 2017].

27 Art. 2.1 LOPD. "Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal: a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento. b) Cuando al responsable del tratamiento no establecido en

También deben ser tenidos en cuenta los informes y las decisiones de las autoridades de control designadas por cada Estado miembro. En España sus funciones corresponden a la Agencia Española de Protección de Datos[28] (en adelante, AEPD), creada en 1992 bajo el auspicio del anterior Convenio 108[29], y convirtiéndose en la figura definida por el Considerando 62 de la Directiva 95/46/CE[30]. Son especialmente relevantes a nuestros efectos su Guía para clientes que contraten servicios de *Cloud Computing*"[31], sus Orientaciones para prestadores de servicios de *Cloud Computing*[32] y su informe Utilización del *Cloud Computing* por

territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público. c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito".

28 Las autoridades competentes en materia de protección de datos desarrollan tareas de información, cooperación y control de acuerdo con las normativas nacionales. Otros muchos países de la Unión Europea poseen instituciones con funciones homólogas a las desempeñadas por nuestra Agencia Española de Protección de Datos. Algunas de ellas han redactado también informes o guías en relación a la computación en la nube, como la española (AEPD, sitio web oficial disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf>); la británica *Information Comissioners Office* (ICO, sitio web oficial disponible en: <https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf>); la francesa *Comission Nationale de l'Informatique et des Libertés* (CNIL, sitio web oficial disponible en: <http://www.cnil.fr/linstitution/actualite/article/article/cloud-computing-cnils-recommandations-for-companies-using-these-new-services>); la sueca *Swedish Data Protection Authority* (DPA, sitio web oficial disponible en: <http://www.datainspektionen.se/in-english/cloud-services/>); la irlandesa *Data Protection Comissioner of Ireland* (PDC, sitio web oficial disponible en: <http://www.dataprotection.ie/docs/03-07-12-Cloud-Computing/1221.htm>); la italiana *Garante per la protezione dei dati personali* (sitio web oficial disponible en: <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906143> o la alemana *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit* (sitio web oficial disponible en: <https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf>). [Fecha de consulta de todos los anteriores sitios web: 9 de mayo de 2017].

29 *Convenio núm. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* [en línea]. Disponible en: <https://www.agpd.es/portalwebAGPD/internacional/textosynormas/textos_consejo_europa/common/PDFs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf>. [Fecha de consulta: 9 de mayo de 2017].

30 Considerando 62 de la Directiva 95/46: "Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales".

31 AEDP. *Guía para clientes que contraten servicios de Cloud Computing* [en línea]. Disponible en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf>. [Fecha de consulta: 9 de mayo de 2017].

32 AEDP. *Orientaciones para prestadores de servicios de Cloud Computing* [en línea].Disponible en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIE

los despachos de abogados y el derecho a la protección de datos de carácter personal[33], así como otra información disponible en su sitio web sobre las obligaciones del responsable del tratamiento, entre las que destacan las exigencias para transferencias internacionales de datos[34].

3.- PRINCIPALES CONCEPTOS DE LA PROTECCIÓN DE DATOS PERSONALES Y SU TRASLADO AL ÁMBITO DE LA COMPUTACIÓN EN LA NUBE

La normativa vigente sobre protección de datos introduce conceptos legales específicos, cuyo contenido consideramos apropiado abordar, en primer lugar, para un mejor estudio de los elementos esenciales que caracterizan la regulación sobre privacidad en Europa y en España; y en segundo lugar, para un mejor estudio del traslado de tales conceptos al contexto de la computación en la nube.

3.1.- Datos personales

La Directiva 95/46/CE pretende garantizar que en todos los Estados miembros la protección del derecho a la intimidad en relación al tratamiento de datos de carácter personal y permitir la libre circulación, dentro del territorio europeo, de estos datos, favoreciendo múltiples actividades económicas[35]. Así lo manifiesta la

---

NTACIONES_Cloud.pdf>. [Fecha de consulta: 9 de mayo de 2017].

33 AEDP. *Informe: Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal* [en línea]. Disponible en: <https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2012/notas_prensa/common/junio/informe_CLOUD.pdf>. [Fecha de consulta: 9 de mayo de 2017].

34 AEPD. *Información sobre transferencias internacionales de datos* [en línea]. Disponible en:. <https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php>. [Fecha de consulta: 9 de mayo de 2017].

35 En la sentencia 292/2000, nuestro Tribunal Constitucional reconoce el carácter fundamental del derecho a la protección de datos. Dice la sentencia, en su fundamento jurídico 2º: "Pues es indudable que los arts. 21.1 y 24.1 y 2 LOPD han regulado el ejercicio de derechos de los individuos que forman parte del haz de facultades que integra el contenido del específico derecho fundamental a la protección de datos personales derivado de los arts. 18.1 y 18.4 CE (...)". El Tribunal Constitucional, en su sentencia 254/1993 (fundamento jurídico 7º) ya admitió que "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". En el fundamento jurídico 4º de su sentencia 173/2011, el Tribunal Constitucional concibe el carácter amplio de este derecho, al afirmar que "el Tribunal Europeo de Derechos Humanos ha venido asumiendo una interpretación extensiva del concepto

propia Directiva en muchos de sus considerandos y en su artículo primero[36].

La LOPD define en el apartado a) de su art. 3 "dato personal" como "*cualquier información concerniente a personas físicas identificadas o identificables*". En particular, a título de ejemplo, los datos que permitan reconocer directa o indirectamente a una persona física pueden hacer referencia a números de identificación (como el DNI o el número de tarjeta sanitaria o de crédito) o a caracteres específicos de su identidad física, fisiológica, mental, económica, cultural o social[37].

La suscripción de servicios de computación en la nube en general implica ingentes cantidades de datos personales: el nombre, la fecha de nacimiento, la dirección postal o de correo electrónico, el número de teléfono, el número de identificación fiscal, etc.[38] Pero también son datos personales las direcciones IP; las *cookies;* las preferencias, gustos o patrones de uso[39]; las etiquetas que permiten las redes sociales[40] o las fotografías de personas identificables, entre otros[41].

«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 este "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". Sin embargo, otros ordenamientos (como el estadounidense) no le conceden tan elevado rango normativo. A pesar que la privacidad se menciona en la Cuarta Enmienda a la Constitución norteamericana, la protección de datos referentes a la intimidad solo entra en juego ante tratamientos gubernamentales abusivos (como regula la *Privacy Act* de 1974) o en la regulación de ciertos sectores como el sanitario o el financiero, que manejan datos de alta sensibilidad. GUERRERO PICÓ, María del Carmen, "El derecho fundamental a la protección de los datos de carácter personal en la Constitución Europea", Revista de Derecho Constitucional Europeo, núm. 4, 2005, págs. 293-332.

36 Directiva 95/46/CE. Art. 1. "Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. 2.Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1".

37 ENISA, *Cloud Security Guide for..., op. cit.*, pág. 28.

38 Para más detalle, podemos acudir al "Dictamen 4/2007 sobre el concepto de datos personales", redactado por el Grupo de Trabajo del Artículo 29 (WP 136) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf>. [Fecha de consulta: 9 de mayo de 2017].

39 LEENES, Ronald, "¿Quién controla la nube?", *Revista de Internet Derecho y Política de la Universitat Oberta de Catalunya*, núm. 11, 2010.

40 Grupo de Trabajo del Articulo 29*, Dictamen nº 5/2009, sobre las redes sociales en línea en sus recomendaciones sobre no publicar fotografías de tercero sin su consentimiento* (WP 163), pág. 8.

41 La política de condiciones del software como servicio de almacenamiento *Dropbox* admite el uso de *cookies* para recabar información y el hecho de que la prestación pueda quedar limitada en caso

La LOPD clasifica los datos personales en tres niveles en función de su sensibilidad, cada uno de ellos asociado a determinadas medidas de seguridad técnicas y organizativas que deberán adoptarse como obligación legal (arts. 80 y 81 RLOPD)[42]. Así, se aplicarán medidas de nivel básico a datos como nombre, apellidos y direcciones de contacto físicas o electrónicas de personas físicas (art. 81.1 RLOPD). Se adoptarán medidas de nivel medio respecto de datos como comisión de infracciones penales o administrativas, solvencia patrimonial, hábitos de consumo, trazos del carácter e información tributaria o financiera (art. 81.2 RLOPD). Por último, tendrán la consideración legal de datos especialmente protegidos (art. 81.3 RLOPD) aquellos que revelen aspectos relativos al origen étnico o racial; creencias religiosas, ideológicas o filosóficas; opiniones políticas; vida sexual; salud o afiliaciones a asociaciones u organizaciones religiosas, filosóficas, políticas o sindicales[43]. Estos datos necesitarán protegerse a través de medidas de seguridad de nivel alto[44].

El nuevo Reglamento 679/2016 define datos personales como "toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador

---

de que no se acepte el uso de esas *cookies*: "*Cookies y otras tecnologías*. Utilizamos tecnologías como las cookies y píxel de seguimiento para proporcionar, mejorar, promocionar y proteger nuestros servicios. Por ejemplo, las cookies nos ayudan a recordar tu nombre de usuario para la próxima visita, entender cómo interactúas con nuestros servicios y mejorarlos a partir de esa información. Puedes configurar tu navegador para que no acepte cookies, pero esto podría limitar tu capacidad para usar los Servicios. (...)". Disponible en: <https://www.dropbox.com/es_ES/privacy>. [Fecha de consulta: 9 de mayo de 2017].

42 El Instituto Nacional de Ciberseguridad INCIBE (anteriormente denominado INTECO), expone en su "Guía para empresas: seguridad y privacidad del Cloud Computing" que habitualmente no será posible que el cliente pueda inspeccionar las medidas de seguridad adoptadas por el proveedor, entre otras razones porque el contrato suscrito será de adhesión. Por este motivo, será fundamental que el cliente se cerciore de que el proveedor se compromete a respetar y cumplir con las obligaciones legales de la LOPD y de la normativa comunitaria. [En línea]. Disponible en: <https://www.incibe.es/protege-tu-empresa/blog/resena-guia-cloud>. [Fecha de consulta: 9 de mayo de 2017].

43 Art. 7 LOPD."(...) Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. (...)".

44 Ver apartado "Medidas de seguridad según la normativa de protección de datos", en este mismo capítulo.

en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"[45]. En cuanto a las medidas de seguridad, el Reglamento europeo establece medidas de seguridad preventivas (privacidad por defecto) a la hora de que las empresas y organizaciones diseñen y creen nuevos productos y servicios que impliquen tratamientos de datos personales; y privacidad por defecto, es decir, la obligación de que las empresas y organizaciones únicamente recaben y traten aquellos datos personales estrictamente necesarios para la actividad que desarrollan, y que esta información no se divulgue a terceros[46].

3.2.- Tratamiento de datos y ficheros

El tratamiento de datos corresponde a aquel conjunto de operaciones automatizadas o no que permitan principalmente recoger, conservar, grabar, modificar, consultar, utilizar, cancelar, bloquear o suprimir datos personales[47].

45 La triple distinción de datos personales efectuada por la LOPD no coincide con la distinción de datos realizada por el nuevo Reglamento General de Protección de Datos, ya que se sigue el mismo mecanismo de la Directiva 95/46, que distinguía únicamente datos personales de carácter general y datos personales de carácter especial. El tratamiento de estos datos, que por su naturaleza son especialmente sensibles (origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, datos genéticos, biométricos dirigidos a identificar, de manera unívoca a una persona física, datos sobre salud o vida u orientación sexual), está prohibido por su artículo 9, aunque este mismo artículo prevé excepciones que levantan esta prohibición (consentimiento explícito del interesado, cumplimiento de obligaciones y ejercicio de derechos del responsable del tratamiento o del interesado por la normativa laboral o de seguridad social, ejercicio de derechos ante tribunales, ejercicio de la medicina, razones de interés público, etc.).

46 Una vez que resulte aplicable el nuevo marco reglamentario, el responsable del tratamiento deberá adoptar las medidas técnicas y organizativas apropiadas para garantizar y demostrar que el tratamiento es conforme al Reglamento (art. 24.1 del Reglamento). En cuanto a estas medidas, el Reglamento distingue entre: a) protección de datos por diseño ("Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados") y b) protección de datos por defecto ("El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas"), en los apartados 1 y 2 del artículo 25 del Reglamento europeo.

47 El artículo 2.b) de la Directiva 95/46 define el tratamiento de datos personales como "cualquier

Especialmente relevantes en la computación en la nube son, entre otros, los tratamientos por almacenamiento de datos, las monitorizaciones de actividades de usuarios, las transferencias y cesiones, y la elaboración de perfiles de actividad o de preferencias con identidades no disociadas.

En relación con los ficheros de datos personales[48], el pequeño empresario, a través del uso de servicios *cloud* y del desarrollo de la relación contractual, puede estar transfiriendo por Internet ficheros (o parte de su contenido) que contengan datos personales de sus clientes, a proveedores *cloud*, tales como listas de correos electrónicos o de contactos, archivos electrónicos almacenados en servidores remotos o cuyo procesamiento tenga lugar a través de software como servicio y en sistemas del proveedor *cloud*, etc.[49] Por ello, el pequeño empresario deberá cumplir las obligaciones de la LOPD, entre ellas, el registro de ficheros, mientras esta normativa

---

operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción". En términos similares lo recogen los artículos 3.c) de la LOPD ("Tratamiento de datos: 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, cesiones y transferencias") y el artículo 5.1.t) del RLOPD ("Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"). El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados, a tenor del artículo 10 de la LOPD, al secreto profesional respecto de esos datos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo: "El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

48 El fichero aparece definido en el art. 5.1.k) del RLOPD como "todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso". Exactamente en los mismos términos aparece recogido en los artículos 2.c) de la Directiva 95/46/CE y 3.b) de la LOPD. El mismo artículo 5.1.k) del RLOPD distingue entre ficheros de titularidad privada y pública, (en atención a quien sea su responsable) y entre ficheros automatizados y no automatizados.

49 A modo de ejemplo, un empresario puede facilitar ficheros con datos personales a proveedores de servicios de correo electrónico y campañas de marketing o comunicaciones masivas electrónicas (*Gmail, Outlook, Mailchimp, TinyLetter...*); servicios de gestión de contactos (*Google contacts, WhatsApp...*) almacenamiento remoto (*Dropbox for Business, Google Drive, Box, iCloud ...*), herramientas de gestión (cualesquiera *Custome Relationship Management* o CRM, como *Salesforce*), etc. El empresario deberá atender a las exigencias de la LOPD para comprobar que estar transferencias de datos son legales, o estará llevando a cabo una infracción grave sancionable con elevadas cuantías.

siga vigente y no se haya realizado aún su adaptación al nuevo Reglamento[50]. Sin embargo, en nuestra opinión, es recomendable que el propio empresario, mediante un asesoramiento adecuado, intente adelantarse a las exigencias del Reglamento y empezar a poner en práctica las principales obligaciones que, de acuerdo con el tipo de tratamiento que lleve a cabo y los riesgos asociados a este, le corresponden como responsable.

3.3.- La asignación de los roles de titular de los datos, responsable y encargado del tratamiento en la computación en la nube

Como es sabido, la normativa sobre protección de datos distingue entre diferentes figuras jurídicas, entre las que destacan el titular de los datos, el responsable del fichero y el encargado del tratamiento, cada uno con distintas responsabilidades asignadas legalmente. En el ámbito del *Cloud Computing,* en la práctica contractual, no se suele asignar ni al proveedor de servicios ni al suscriptor la condición de responsable o encargado del tratamiento de forma expresa.

Como veremos, aunque las autoridades en materia de protección de datos coinciden en que el prestador de servicios *cloud* es un mero encargado del tratamiento, y la empresa suscriptora es responsable de los datos personales que le

50 Con la actual Ley Orgánica de Protección de Datos de Carácter Personal, estos ficheros deben inscribirse en el Registro General de Protección de Datos, órgano que forma parte de la AEPD, que pretende garantizar el ejercicio de los derechos de información, acceso, rectificación, oposición y cancelación de datos de los art. 14 a 17 LOPD, por parte de sus titulares, y encargado también de tramitar las autorizaciones para la transferencia internacional de datos personales. Así lo establece el art. 55 del RLOPD. Sin embargo, quedan excluidos de tal inscripción aquellos mencionados expresamente en el art. 2.2 de la LOPD, como son los ficheros mantenidos por personas físicas para actividades domésticas o personales. No solicitar la inscripción de ficheros de carácter personal constituye infracción leve, de acuerdo con el art. 44.2.b de la LOPD. No obstante, el nuevo Reglamento 679/2016 General de Protección de Datos elimina la obligación de notificación de ficheros a las autoridades de control, dado el escaso beneficio y alto coste administrativo de este procedimiento (tal y como afirma el considerando 89 del Reglamento) y compensa esta obligación a través de otros sistemas que considera más efectivos para maximizar la protección de datos de los interesados y el cumplimiento legal, como por ejemplo la evaluación de impacto a modo de análisis previo de riesgos (considerando 90 y arts. 35 y 36 del Reglamento), la obligación de notificar violaciones de seguridad (arts. 33 y 34 del Reglamento), el rendimiento de cuentas ante la autoridad nacional y, eventualmente, ante el Comité Europeo de Protección de Datos, el fomento de la adopción de códigos de conducta y mecanismos de certificación de cumplimiento con la normativa de protección de datos (arts. 40 a 43 del Reglamento), y la llevanza de un registro de todas las actividades, entre otros.

transfiere, nosotros opinamos que estas calificaciones no siempre concuerdan con la actividad real de manejo y control efectivo sobre el tratamiento de los datos personales migrados, como veremos con más detalle en los pertinentes apartados[51].

3.3.1.- El titular de los datos y la prestación de consentimiento informado e inequívoco

El titular de los datos de carácter personal es aquel afectado o interesado por los datos que sean objeto de tratamiento, puesto que suponen información que le concierne como persona física identificada o identificable[52].

Dice la propia LOPD en su art. 1 que "la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar". De aquí que sea esencial la información y el consentimiento por parte del titular de los datos ante la recogida de estos, como veremos a continuación.

En primer lugar, cuando al interesado se le soliciten datos personales, tiene derecho a ser informado de manera previa sobre el tratamiento al cual van a someterse esos datos. Este derecho a la información, que aparece recogido en el artículo 5 de la LOPD, supone que en el momento de registrarse los datos personales para poder tratarlos, se informará a su titular "de modo expreso, preciso e inequívoco: a) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información[53]; b) del carácter obligatorio o facultativo de su respuesta a las preguntas que

---

51 Es habitual encontrar, en los contratos de adhesión destinados a empresarios, cláusulas como la siguiente: "El cliente es el único responsable de: (i) cualquier uso para el que se empleen los servicios; o (ii) el incumplimiento de cualquier norma que pudiera resultar aplicable a causa o en relación con la utilización de los Servicios, incluyendo sin carácter limitativo, las normas de uso de los servicios objeto del presente contrato, las disposiciones en materia de protección de datos, comunicaciones internacionales, propiedad intelectual, exportación de información tecnológica, protección de consumidores y usuarios, confidencialidad, secreto de las comunicaciones y derecho a la intimidad. En este sentido, el cliente se obliga a adoptar las medidas oportunas para evitar cualquier intromisión ilegítima en la intimidad de las personas físicas o jurídicas o que suponga violación del derecho al honor de terceros". Fuente: condiciones generales de los servicios Claranet [en línea]. Disponible en: <http://www.claranet.es/legal>. [Fecha de consulta: 10 de mayo de 2017].Con este tipo de cláusulas, se sobreentiende que la responsabilidad por los datos personales migrados recae sobre el cliente, y que la función del proveedor es únicamente procesarlos. Esta posición jurídica de encargado es la que el proveedor preferirá asumir en caso de duda, porque implica menores responsabilidades y obligaciones que la categoría de responsable.

52 Esta acepción de "titular de los datos" puede deducirse de las definiciones de "datos personales" y de "afectado o interesado" recogidas por el art. 3 de la LOPD. La LOPD define al "interesado o afectado" como "persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo".

53 El tema de los destinatarios de la información se tratará más detenidamente en este mismo

les sean planteadas; c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y e) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Esta información se facilitará a través del medio que se utilice para la recogida de los datos que vayan a ser objeto del tratamiento y para la obtención de su consentimiento".

Si bien la AEPD define en su sitio web al destinatario o cesionario como "la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen datos", y la cesión o comunicación de datos aparece definida en el artículo 3 de la LOPD como "tratamiento de datos que supone su revelación a una persona distinta del interesado", quedan excluidos del concepto de destinatarios los encargados del tratamiento, puesto que no se trata de una comunicación de datos, tal y como reconoce el art. 12.1 de la LOPD: "No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento"[54]. Como veremos más adelante, en la mayoría de casos el papel de encargado del tratamiento corresponderá al proveedor de servicios de computación en la nube que presta sus servicios al pequeño empresario, y este último asumirá generalmente el papel de responsable del fichero. De lo anterior puede desprenderse que no resulta necesario, con la actual redacción de la LOPD, que en el momento de recabarse los datos se informe al titular de los datos de que estos parte o todo su tratamiento pueda efectuarse mediante servicios de computación en la nube, aunque lo anterior suponga una transferencia internacional de datos[55].

---

apartado, junto con otros roles, y con las transferencias internacionales de datos, en este mismo capítulo.

54 Art. 12 LOPD. "1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. 2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar. 3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. 4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".

55 Todo ello sin perjuicio del cumplimiento de las exigencias legales respecto de las transferencias internacionales de datos personales. Ello es así porque en aquellos casos en los que tenga lugar una transferencia internacional de datos personales (a falta de otras definiciones, de acuerdo con la efectuada por el artículo 5.1.s de nuestro RLOPD: "tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del

El nuevo Reglamento europeo también exige al responsable del tratamiento que facilite cierta información (art. 12), la cual variará dependiendo de si los datos personales se obtienen directamente del interesado (art. 13) o no (art. 14).

Existen diferencias entre las regulaciones de la actual LOPD y del Reglamento europeo, obligando el Reglamento a una información más completa y exigente. Cuando el Reglamento europeo sea aplicable, el derecho de información al interesado supondrá facilitarle cierta información relacionada con tratamientos mediante *Cloud Computing*, como la intención de realizar transferencias de datos a terceros países (por ejemplo, el alojamiento de datos en sistemas remotos situados fuera de las fronteras europeas) y a que se detallen las garantías relacionadas con tales transferencias internacionales; en su caso, los datos de contacto del delegado de protección de datos; el plazo de conservación de los datos (lo cual supondrá realizar averiguaciones sobre los sistemas de conservación y borrado de datos por parte del proveedor *cloud*); la existencia de los derechos del interesado (que incluirá información sobre los nuevos derechos de limitación al tratamiento y portabilidad y a reclamar ante una autoridad de control); si esa comunicación de datos es un requisito legal o contractual y de las consecuencias de no facilitar esos datos; de la elaboración de perfiles automatizados y sus consecuencias para el interesado (por ejemplo, por razones de mejora de la mercadotecnia); e información sobre otros fines a los cuales puedan destinarse esos datos una vez finalizada la finalidad inicial que motivó su recolección. Asimismo, también deberá informarse al interesado de la base jurídica que permite tratar sus datos personales, tal y como exige el artículo 13.1.f) del Reglamento europeo[56].

---

fichero establecido en territorio español", y con lo establecido en los artículos 25: "Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado" y 26.2 de la Directiva 95/46/CE: "los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas"), no será relevante el hecho de que se trate de una cesión o comunicación de datos, siempre y cuando el tratamiento de datos tenga lugar por cuenta de un responsable del fichero establecido en territorio español. Ver apartado "Transferencias internacionales de datos y *Cloud Computing*", en este mismo capítulo.

56 Artículo 13. 1. f) del Reglamento General de Protección de Datos: "1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación: (...) f) en su caso, la intención del

Una vez el interesado ha sido adecuadamente informado de acuerdo con las exigencias legales, este deberá consentir el tratamiento de sus datos personales. En su artículo 5. d), la LOPD define el consentimiento del titular como "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen", y en su artículo 6 se exige el consentimiento inequívoco del titular para realizar el tratamiento de datos[57]: "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa"[58].

En los entornos en la nube, de acuerdo con la vigente LOPD, al no ser necesario que informe al titular en relación a la transferencia de estos datos a sistemas de un proveedor *cloud* con la finalidad de procesarlos o almacenarlos remotamente, tampoco será necesario que obtenga su consentimiento sobre ese tratamiento efectuado en la nube, puesto que, al considerarse generalmente al proveedor *cloud* un encargado del tratamiento (como veremos más adelante), no nos hallaremos, como se ha dicho, ante una comunicación de datos, tal y como considera el ya mencionado artículo 12.1 de la LOPD.

Por otra parte, el art. 6.1 de la LOPD exige que el consentimiento sea inequívoco. El Dictamen 15/2011 sobre la definición del consentimiento del Grupo de Trabajo del Artículo 29 aclara el significado de la expresión "inequívoco", término igualmente recogido en el mismo sentido en el art. 7.a) de la Directiva 95/46/CE[59].

---

responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado. (...)".

57 En el art. 6.2 de la LOPD se establecen excepciones a esta obligación de requerir el consentimiento: "No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado (...), o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

58 El Tribunal Constitucional afirma que el consentimiento eficaz del titular de los datos permite a terceros el acceso a cierta información relativa a su ámbito de intimidad personal y familiar (sentencias del Tribunal Constitucional 159/2009, de 29 de junio, y 173/2011, de 7 de noviembre). Añade, además, que cuando el tratamiento de los datos se realiza con objetivos diferentes a aquellos para lo cuales se otorgó el consentimiento del titular, se está infringiendo el derecho fundamental a la intimidad (sentencias del Tribunal Constitucional 173/2011, de 7 de noviembre, 70/2009, de 23 de marzo, y 206/2007, de 24 de septiembre).

59 Art. 7 a) Directiva 95/46/CE: "Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca (...)".

Dictamina el Grupo de Trabajo del Artículo 29 que el procedimiento de obtención y otorgamiento no debe dejar ninguna duda sobre la intención del interesado de prestar su consentimiento, y pone como ejemplos una forma manuscrita en un formulario en papel, un consentimiento oral o un comportamiento del interesado que permita deducir tal intención.

Así, de acuerdo con la actual LOPD, no sería válida la obtención de un consentimiento implícito, basado en el silencio. Lo mismo puede desprenderse del mencionado Dictamen, porque el Grupo de Trabajo del Artículo 29 exige, para la adecuación del consentimiento a las exigencias de la Directiva 95/46/CE, una acción expresa de la persona. Además, anima a los responsables del tratamiento (y en la computación en la nube, nosotros lo consideramos extensible a los proveedores-encargados) a que adopten "medidas y procedimientos pertinentes para demostrar que se ha dado el consentimiento. Cuanto más complicados sean los entornos en los que actúan, más medidas serán necesarias para garantizar que el consentimiento puede demostrarse"[60]. Y en sus conclusiones, se aclara en el mismo Dictamen que "la utilización de opciones por defecto que el interesado debe modificar para negarse al tratamiento (consentimiento basado en el silencio) no constituye consentimiento inequívoco. Así sucede sobre todo en el contexto en línea"[61].

Esta propuesta podría aplicarse, como considera el Grupo de Expertos de la *Cloud Computing Strategy* en su *Discussion Paper* sobre cláusulas abusivas, a aquellos cambios en las políticas de privacidad que se entienden aceptadas de forma implícita si el usuario sigue utilizando el servicio, puesto que el usuario no tiene otra opción que aceptar estas condiciones si quiere seguir disfrutando de la prestación[62].

En otro Dictamen, concretamente en el Dictamen sobre los conceptos de responsable del tratamiento y encargado del tratamiento", el Grupo de Trabajo del Artículo 29 propuso en su momento mecanismos idóneos para recabar el consentimiento en línea[63]. Puso como ejemplos la introducción de casillas visibles en

60 Dictamen 15/2011 del GT29 (WP 187) sobre definición del consentimiento, pág 28.

61 Dictamen 15/2011 del GT29 (WP 187) sobre definición del consentimiento, pág 40.

62 *Discussion Paper* sobre cláusulas abusivas del Grupo de expertos de la Comisión Europea en contratos de *Cloud Computing* [en línea], pág 7. Disponible en: <http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_unfair_contract_terms_en.pdf>. [Fecha de consulta: 10 de mayo de 2017]. El grupo de expertos pone como ejemplo los cambios en la política de privacidad de Google en marzo de 2012, donde no se requirió el consentimiento explícito a los consumidores, y estos no tenían posibilidad real de oponerse a los cambios, con lo cual quedaban vinculados inapelablemente por la nueva política. Como resultado, el consentimiento dejaba de ser libre en este caso.

63 Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del

los formularios que el interesado deberá marcar para considerar otorgado ese consentimiento explícito[64], el envío de mensajes electrónicos de confirmación o la activación de iconos, etc., siempre que ello permita, de acuerdo con el considerando 17 de la Directiva 95/46/CE, "la manifestación libre, inequívoca y fundada de la voluntad del usuario, por ejemplo mediante la selección de una casilla de un sitio web en Internet".

En ocasiones, como hemos observado, puede deducirse de ciertas acciones que el interesado ha prestado su consentimiento. Igualmente, el Grupo de Trabajo se refiere a la importancia de la transparencia y a la necesidad de un consentimiento informado como requisitos de validez del consentimiento exigido por la Directiva 95/46/CE[65]. Implica que toda la información necesaria debe facilitarse en el momento en que se solicita el consentimiento, y aunque en principio debe abarcar los contenidos del art. 10 de la Directiva, el mismo Dictamen reconoce que "también depende del momento y las circunstancias en las que se solicite el consentimiento"[66]. El Dictamen también pone de manifiesto el requisito de que este consentimiento sea específico, es decir, debe ser comprensible y referirse de manera clara y precisa al alcance y las consecuencias del tratamiento de datos. El Grupo de Trabajo interpreta que el individuo afectado debe contar "con información exacta y completa, dada de forma clara y comprensible, sobre todas las cuestiones pertinentes, en especial las especificadas en los art. 10 y 11 de la Directiva", como la naturaleza de los datos, los fines del tratamiento, los destinatarios y los derechos del interesado.

La aplicación del nuevo Reglamento europeo supone como se ha dicho, cambios relevantes respecto del derecho de información del interesado, así como la necesidad de una manifestación proactiva del consentimiento para que se entienda como expreso, como veremos a continuación. En primer lugar, con la nueva norma será necesario que el interesado, tras haber sido adecuadamente informado,

---

tratamiento" del Grupo de Trabajo del Artículo 29 (WP 169) [en línea], pág. 36. Disponible en: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf>. [Fecha de consulta: 10 de mayo de 2017].

64 Dictamen 15/2011 del GT29 (WP 187) sobre definición del consentimiento, págs. 25 y 29.

65 Dictamen 15/2011 del GT29 (WP 187) sobre definición del consentimiento, pág. 25.

66 Art. 10 Directiva 95/46/CE. "Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como: los destinatarios o las categorías de destinatarios de los datos, el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado".

consienta sobre potenciales tratamientos de sus datos personales a través de servicios de computación en la nube cuando esa comunicación al proveedor *cloud* suponga una transferencia internacional de datos personales, junto con las garantías legales de esa transferencia, de acuerdo con el artículo 13. 1.f) del Reglamento europeo. El artículo 7.1 del Reglamento europeo exige al responsable que pueda probar ese consentimiento[67].

En segundo lugar, el nuevo Reglamento europeo no admite el consentimiento tácito del interesado en el tratamiento de datos. Así, se exige un consentimiento expreso, que, como informa en su Considerando 32, supondrá un acto afirmativo claro, informado e inequívoco, como una declaración por escrito, marcar una casilla de un sitio web, o una declaración verbal, y no habrá consentimiento válido en el caso de casillas premarcadas, el silencio o la inacción[68].

Por otro lado, el consentimiento como manifestación de voluntad informada es especialmente importante en el contexto de las transmisiones de datos personales a terceros países, como veremos en posteriores apartados.

Por último, cabe decir que el interesado puede revocar su consentimiento

67 Artículo 7 del Reglamento General de Protección de Datos. "1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales". Asimismo, el considerando 42 del mismo Reglamento afirma: "Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo, debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno".

68 Considerando 32 del Reglamento General de Protección de Datos: "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta".

sobre el tratamiento en cualquier momento, tal y como se reconoce en el art. 3 de la LOPD, como ha ratificado el Tribunal Constitucional[69] y como establece, a modo de derecho, el artículo 7.3 del nuevo Reglamento europeo[70]. En los entornos de la nube, esta revocación, así como el ejercicio del derecho de cancelación de datos, tiene dificultades en cuanto a su materialización, debido, principalmente, a la ubicación remota de los datos, a su replicado, a la intervención de múltiples subproveedores y a la falta de mecanismos puestos a disposición por el proveedor o proveedores para que la revocación sea materialmente realizada[71]. El nuevo Reglamento obliga, sin embargo, al responsable (y, en su caso, al encargado del tratamiento), no solo a facilitar al interesado el ejercicio de este derecho, sino a que sea "tan fácil retirar el consentimiento como darlo" (art. 7.3 del Reglamento europeo *in fine*).

El interesado deberá ejercer este derecho ante el responsable, quien será el encargado de materializar tal revocación. Ello es así puesto que no es obligatorio que el interesado tenga conocimiento o que preste su consentimiento para que el responsable pueda subcontratar a un encargado del tratamiento, de acuerdo con el art. 12.1 LOPD[72] (aunque sí deberá estar informado, una vez que el nuevo Reglamento europeo sea aplicable, en el caso de que esta subcontrata implique una transferencia internacional de datos). A menudo, la subcontratación tiene lugar entre un empresario (responsable del tratamiento de los datos de sus clientes) que suscribe los servicios del proveedor *cloud* (encargado del tratamiento). En opinión del Grupo de Trabajo del Artículo 29[73], a la que nos adherimos, el proveedor *cloud*, como encargado del tratamiento, deberá facilitar al responsable el ejercicio de este derecho del titular de los datos, de acuerdo con la delegación que sustenta el contrato entre responsable y encargado del tratamiento o entre exportador e

69 Sentencias del Tribunal Constitucional 159/2009, de 29 de junio, y 173/2011, de 7 de noviembre.

70 Artículo 7.3 del Reglamento General de Protección de Datos. "El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo".

71 De esta revocación podrán derivarse acciones como el borrado de datos personales afectados que se encuentren en los sistemas del proveedor, Para ello, ver apartado "Los efectos de la finalización del contrato de computación en la nube sobre los datos personales", en este mismo capítulo.

72 Art. 12.1 LOPD. "No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento".

73 Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" (WP 169) [en línea]. Disponible en: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf>. [Fecha de consulta: 10 de mayo de 2017].

importador de datos de carácter personal[74].

Esta obligación del encargado de asistir al responsable en cuanto a la atención de solicitudes del interesado se recoge en el Reglamento en el artículo 28.3.e)[75], y la obligación del responsable de atender a las peticiones del interesado en cuanto al ejercicio de sus derechos respecto de los datos personales que le conciernen y su tratamiento, en el artículo 12.2 de la misma norma[76].

3.3.2.- El responsable del tratamiento

El responsable del tratamiento es aquella persona física o jurídica (pública, privada u órgano administrativo) que decida sobre la finalidad, contenido y uso del tratamiento (art. 3. d de la LOPD y art. 2.d de la Directiva 95/46/CE)[77], y que,

74 Dice el Dictamen 1/2010 del Grupo de Trabajo del Art. 29 que "El elemento más importante es el que establece que el encargado del tratamiento actúa «por cuenta del responsable del tratamiento». Actuar en nombre de alguien significa servir los intereses de otro y remite al concepto legal de «delegación». En el caso de la normativa de protección de datos, el encargado del tratamiento está llamado a aplicar las instrucciones dadas por el responsable del tratamiento, cuando menos en lo relativo a los fines del tratamiento y a los elementos esenciales de los medios (...). Ahora bien, la delegación aún puede implicar un cierto grado de discrecionalidad sobre cómo servir mejor los intereses del responsable del tratamiento, permitiendo que el encargado del tratamiento elija los medios técnicos y de organización más adecuados".

75 Artículo 28.3 del Reglamento General de Protección de Datos. "3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado: (...) e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III".

76 Artículo 12.2 del Reglamento General de Protección de Datos. "El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado".

77 El Reglamento General de Protección de Datos introduce en su artículo 4 el concepto de "medios del tratamiento" para identificar al responsable: "«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros". Entendemos, pues, que es el responsable quien decide si el tratamiento tendrá lugar de manera manual o automatizada, en qué operaciones consistirá ese tratamiento (recogida, registro, organización, estructura, conservación, comunicación, destrucción, etc.) y cómo se llevarán a cabo. Al respecto, nos remitimos a ÁLVAREZ HERNANDO, Javier, " Acceso a datos por cuenta de terceros. El encargado del tratamiento y su régimen jurídico. Servicios de Cloud Computing", *Grandes Tratados. Prácticum Protección de datos*, 1ª Edición, Navarra, 2015, págs. 167-204.

además, disponga los medios para llevarlo a cabo (el pequeño empresario decide sobre la elección de los mecanismos que utilizará para efectuar el tratamiento de los datos personales: documentos físicos, uso de software alojado en sus propios equipos o, en el caso que nos ocupa, uso de servicios de computación en la nube para tratar datos personales de terceros). Su designación es relevante por dos motivos: el primero, como uno de los criterios que determinan la aplicabilidad de la vigente Directiva 95/46/CE y de una concreta legislación nacional al tratamiento de datos, así como del Reglamento europeo todavía no aplicable[78]; el segundo, porque se le asignan ciertas responsabilidades y obligaciones legales, entre ellas facilitar el ejercicio de los derechos del interesado en relación al tratamiento.

De forma general, el Dictamen 1/2010 del Grupo de Trabajo del Artículo 29 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" reconoce que, sin una adecuada distribución de responsabilidades, las disposiciones legales pueden resultar ineficaces en la práctica[79]. En sus conclusiones, este Dictamen afirma que la determinación de los medios del procesamiento y otras cuestiones técnicas u organizativas pueden ser delegadas del responsable al encargado del tratamiento, pero que las cuestiones de fondo que resulten esenciales en cuanto a la legitimidad del tratamiento (como los datos que deban tratarse, la recogida del consentimiento del titular, la duración de su conservación, el acceso, etc.) deben ser

78 Para más detalles, podemos acudir al Dictamen del GT29 8/2010 sobre ley aplicable. En cuanto al ámbito de aplicación territorial de la LOPD y del RLOPD, acudiremos a sus arts. 2.1 ("La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado. Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal: a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento. b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público. c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito"). Por otra parte, el Reglamento General de Protección de Datos se aplicará a aquellos responsables y encargados que tengan sus establecimientos en la Unión Europea, aunque el tratamiento se realice en otras localizaciones, tal y como afirma su artículo 3.1 ("1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. "). Además, el Reglamento europeo utiliza otros criterios de aplicación territorial que resultan en un destino más extenso de los efectos de la norma, en comparación con la Directiva 95/46/CE.

79 Dictamen 1/2010 del GT29 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" (WP 169) [en línea], pág. 1. Disponible en: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf> [Fecha de consulta: 10 de mayo de 2017].

determinadas por el responsable[80].

Asimismo, considera el mismo Dictamen 1/2010 del Grupo de Trabajo del Artículo 29 que "El concepto de responsable del tratamiento es autónomo, en el sentido de que debe interpretarse fundamentalmente con arreglo a la legislación comunitaria de protección de datos, y funcional, en el sentido de que su objetivo es asignar responsabilidades en función de la capacidad de influencia de hecho, y, por consiguiente, se basa en un análisis de los hechos más que en un análisis formal"[81]. Por ello, para una adecuada delimitación de responsabilidades en cuanto al tratamiento de datos personales se deben tener en cuenta, además de las relaciones jurídicas existentes entre el interesado, el responsable y los eventuales encargados, el análisis de las situaciones fácticas que tienen lugar en cada caso[82].

---

80 "El hecho de determinar los «fines» del tratamiento trae consigo la consideración de responsable del tratamiento (de facto). En cambio, la determinación de los «medios» del procesamiento puede ser delegada por el responsable del tratamiento en la medida en que se trate de cuestiones técnicas u organizativas. Sin embargo, las cuestiones de fondo que sean esenciales a efectos de la legitimidad del tratamiento —como los datos que deban tratarse, la duración de su conservación, el acceso, etc.— deben ser determinadas por el responsable del tratamiento". Dictamen 1/2010 del GT29 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", *op. cit.*, pág. 36.

81 En concreto nos referimos al apartado titulado "Observaciones generales y cuestiones políticas. Contexto pertinente" del Dictamen 1/2010 del GT29 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" (WP 169) [en línea]. Disponible en: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_es.pdf>. [Fecha de consulta: 10 de mayo de 2017].

82 El propio Grupo de Trabajo reconoce, en las conclusiones del mismo Dictamen 1/2010, las dificultades que conlleva en la práctica asignar estas definiciones, puesto que "caben muchas situaciones hipotéticas que impliquen la actuación de responsables y encargados del tratamiento, solos o conjuntamente, y con distintos grados de autonomía y responsabilidad". En este mismo Dictamen 1/2010, de ámbito general, el Grupo de Trabajo del Artículo 29 adelantaba la dificultad de distinguir responsabilidades especialmente en entornos en la nube y en servicios de red social: "En el otro extremo han surgido cuestiones nuevas y complejas relacionadas con el uso de la informática distribuida, en particular la «computación en la nube» y la «informática en malla (grid)" (Dictamen 1/2010 (WP 169), *op. cit.*, pág. 7). Asimismo, en el Dictamen 5/2009 sobre las redes sociales en línea (WP 163) el Grupo de Trabajo del Artículo 29 ilustra la distribución de responsabilidades entre proveedor *cloud* de red social y usuario doméstico (es decir, que actúa como consumidor y a la vez como titular de los datos, y se pone en contacto con personas que forman parte de su ámbito personal, familiar o doméstico), determinando que en este caso, el proveedor cuyos servicios ha contratado directamente un titular de datos personales, y que trata esos datos personales de su usuario, está actuando como responsable del tratamiento. El objeto de nuestro trabajo se basa en los supuestos en los que un pequeño empresario contrata con el proveedor *cloud* la prestación de un servicio de procesamiento o almacenamiento de datos, que podrá utilizar, entre otros fines, para tratar datos de carácter personal. En estos casos, la distribución de las cargas entre el pequeño empresario y el proveedor *cloud* parece sencilla, de acuerdo con el Dictamen 5/2009 sobre redes sociales en línea, y el Dictamen 5/2012, correspondiendo al primero la condición de responsable del tratamiento según la normativa, y al segundo la condición de encargado del tratamiento. Sin embargo, la distribución de responsabilidades entre ambos no siempre estará exenta de problemas, como se verá en posteriores apartados. Para más información sobre la distribución de responsabilidades en

Dentro del ámbito de la computación en la nube, el Dictamen 5/2012 sobre el *Cloud Computing* del Grupo de Trabajo del Art. 29 interpreta que, puesto que el empresario suscriptor de servicios en la nube es quien define el propósito del tratamiento y la externalización de todo o parte de este tratamiento, este cliente *cloud* está actuando como responsable del tratamiento, y como tal, debe asumir su parte de responsabilidad y su sujeción a todos los deberes legales derivados principalmente de la Directiva 95/46/CE[83]. Por lo tanto, considera que la

materia de protección de datos en el ámbito de las redes sociales, podemos acudir al referido Dictamen 5/2009 sobre las redes sociales en línea, del Grupo de Trabajo del Art. 29 [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf>. [Fecha de consulta: 10 de mayo de 2017]. Asimismo, nos remitimos a APARICIO VAQUERO, Juan Pablo "Cuestiones de derecho aplicable y responsabilidad de los prestadores de servicios de red social y de sus usuarios", *En torno a la privacidad y la protección de datos en la sociedad de la información* (Coord. Juan Pablo Aparicio, Alfredo Batuecas), Granada, 2015, págs. 187 a 231.

83 En cuanto a las obligaciones del responsable del tratamiento, se desprende de la LOPD y del RLOPD que el cliente (en nuestro caso, el pequeño empresario), como responsable: a) puesto que es quien determina el propósito del tratamiento antes de recabar los datos (y debe garantizar que no se procesarán los datos con propósitos diferentes a aquellos por los cuales se recabaron, excepto que exista consentimiento), debe informar al interesado de los extremos del artículo 5 LOPD (existencia de un fichero o del tratamiento de datos personales, de la identidad del responsable, etc.) de manera expresa, precisa e inequívoca. Además, deberá recabar su consentimiento de manera inequívoca, salvo que la ley disponga lo contrario, (art. 6 LOPD); b) debe notificar, previamente a su creación y a cualquier tratamiento de datos, la existencia de un fichero con datos de carácter personal, independientemente del sistema de tratamiento empleado y del soporte, sea automatizado o no (arts. 25 y 26 LOPD; y 55.2 y 56 RLOPD), e inscribir en el Registro General de Protección de datos los ficheros y las autorizaciones de transferencias internacionales de datos de carácter personal con destino a países que no presten un nivel de protección equiparable al que presta la LOPD (obligación que persistirá hasta que resulte aplicable el nuevo Reglamento europeo); c) debe implementar una política de seguridad que incluya análisis de riesgos, instrucción del personal, implementación de planes que permitan una rápida reacción y recuperación de datos ante incidentes de seguridad (arts. 9.1 y 12.1 LOPD, y 90 RLOPD); d) debe instaurar medidas de seguridad físicas y lógicas para proteger sus sistemas informáticos; y tiene la obligación de elegir un proveedor de servicios *cloud* que implemente las medidas de seguridad adecuadas(arts. 9.1, 12.1 y 12.2 LOPD; y 79 RLOPD); e) recogerá por vía contractual la habilitación del encargado para el tratamiento de datos personales, que se llevará a cabo bajo las instrucciones y por cuenta del responsable (12.2 LOPD) y redactará el pertinente documento de seguridad (art. 88 RLOPD); f) deberá facilitar información sobre si existe subcontratación, la identidad de los subcontratados o la finalidad de la subcontratación, y en su caso, habilitarlos a su vez para subcontratar (art. 12 LOPD, y arts. 20.2 y 21.2 RLOPD), así como el lugar donde se procesan los datos en caso de eventuales transferencias internacionales (arts. 65 a 70 RLOPD); g) está obligado a inspeccionar el tratamiento de datos que realizan los encargados y subencargados (art. 20.2 y 21 RLOPD); h) estará informado sobre las medidas de seguridad técnicas y organizativas adoptadas por el proveedor (encargado) y ser notificado sobre incidentes de seguridad que puedan afectar a datos personales (art. 20.2 RLOPD); i) debe poder demostrar el cumplimiento de la normativa, en especial la relacionada con las medidas de seguridad de los datos

introducción de una cláusula contractual que intente desplazar la calificación de responsable del tratamiento al proveedor no tendrá validez jurídica, por ser contraria a la Directiva 95/46/CE y, en nuestro caso, a la Ley Orgánica de Protección de Datos.

Sin embargo, a pesar de esta categorización global del empresario suscriptor de servicios *cloud* como responsable, debe tenerse en cuenta su capacidad de control efectivo sobre el tratamiento, en cuanto sufre una considerable merma desde el momento en el que introduce datos personales de terceros en la nube, por lo que será sumamente necesario, para mantener la categorización del cliente *cloud* empresario como responsable del tratamiento y proveedor *cloud* como encargado, que este último permita al responsable el cumplimiento de sus obligaciones como tal, poniendo a su disposición los mecanismos necesarios para facilitar esta labor, y se someta a sus instrucciones respecto del tratamiento de los datos de carácter personal facilitados. Por lo anterior, coincidimos con el Grupo de Trabajo en que deben matizarse las responsabilidades del cliente de servicios de computación en la nube y consideramos que deben plantearse mecanismos complementarios que compensen la imposibilidad práctica de control pleno del tratamiento que realiza el proveedor *cloud*[84].

El nuevo Reglamento europeo, para favorecer el cumplimiento legal en las operaciones de tratamiento de responsables y encargados, fomenta la adopción de códigos de conducta supervisados y la creación de mecanismos de certificación, sellos y marcas en materia de protección de datos[85]. Regula los procedimientos de

---

(art. 20.2 RLOPD) j) puede quedar total o parcialmente exento de su responsabilidad si prueba que no ha sido responsable del evento que ha causado el daño, y que ha adoptado la diligencia oportuna que le era exigible (127.f RLOPD); y k) una vez extinguido el contrato (de forma ordinaria o extraordinaria, y con o sin preaviso), debe asegurar la recuperación de datos, la transición a otro proveedor y el borrado efectivo de todas las réplicas obrantes en la cadena de subproveedores (art. 12.3 LOPD y 22.1 RLOPD).

84 Nos sumamos a la opinión de RUBÍ NAVARRETE, cuando propone que las fórmulas alternativas sean jurídicamente vinculantes, permitan a las autoridades de control ejercer sus competencias, y que incorporen opciones que permitan a los titulares de datos ejercer sus derechos y obtener compensaciones en caso de vulnerarse sus garantías. RUBÍ NAVARRETE, Jesús, "El proveedor de *cloud* como encargado del tratamiento", en *Derecho y Cloud Computing*, (Coord. Ricard Martínez), 1ª edición, Navarra, 2012, pág. 101.

85 Así lo enuncian los considerandos del Reglamento General de Protección de Datos 98 ("Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se

creación de códigos, certificados y sellos en sus artículos 40 a 43[86], los cuales podrán suscribirse de forma voluntaria por los proveedores *cloud,* serán expedidos con validez periódica y su adopción será un criterio a tener en consideración en cuanto a la imposición de eventuales sanciones (art. 83.2.j) del Reglamento europeo)[87].

Asimismo, el nuevo Reglamento europeo mantiene la obligación para el responsable de implementar medidas técnicas y organizativas conformes con la naturaleza, el ámbito, el contexto y los fines del tratamiento, y adecuados a la probabilidad y gravedad de los riesgos que puedan suponer para los derechos y libertades de los titulares de los datos (art. 24.1). Entre estas medidas se encuentra la adopción de una adecuada política de protección de datos (art. 24.2)[88]. Por ello, muchas de las obligaciones recogidas para el responsable en la normativa española (LOPD y RLOPD) seguirán siendo compatibles o coincidentes con las disposiciones del nuevo Reglamento cuando este sea aplicable[89].Además, el nuevo Reglamento incorpora otras obligaciones añadidas para el responsable del tratamiento[90].

---

derive del tratamiento") y 100 ("A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes").

86 Estos artículos serán objeto de un análisis más detallado en posteriores apartados de este miso capítulo.

87 Artículo 83.2.j) del Reglamento General de Protección de Datos. "Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta: (...) j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42".

88 Reglamento General de Protección de Datos. Artículo 24: "1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario. 2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos. (...)".

89 Entre las medidas técnicas y organizativas que puede aplicar el responsable, el Reglamento distingue la protección de datos desde el diseño del tratamiento, es decir, adoptadas desde el momento de determinar los medios de tratamiento como durante la realización de este, que incluye medidas como la seudonimización o la minimización de datos; y la protección de datos por defecto, que garanticen únicamente el tratamiento de aquellos datos estrictamente necesarios para cada uno de los fines específicos, en cuanto a cantidad, extensión de su tratamiento, período de conservación y accesibilidad limitada (arts. 25.1 y 25.2). Para acreditar la implementación de estas medidas, el responsable puede contar con mecanismos de certificación (art. 25.3 del Reglamento europeo).

90 Primeramente, obliga a la llevanza de un registro de las actividades de tratamiento que contendrá, entre otros, el nombre y los datos de contacto del responsable, corresponsable, representante en la

3.3.3.- El encargado del tratamiento

Como hemos mencionado, el responsable del tratamiento decidirá si trata los datos dentro de su organización o bien si subcontrata todo o parte de ese tratamiento. Fruto de este encargo o subcontratación nacerá un nexo entre el responsable y la figura jurídica del encargado, que aparece definida en el art. 2 de la Directiva 95/46/CE (en los mismos términos, en el art. 3 de la LOPD, y en términos muy similares, el art. 4.8 del Reglamento General de Protección de Datos[91]) como: "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

De esta distinción entre las categorías de responsable y encargado del tratamiento, y dado que el encargado actúa bajo las instrucciones del responsable, se derivarán cuestiones legales importantes, como la correspondiente distribución de obligaciones en materia de seguridad o quién debe responder en caso de que se produzcan infracciones de la norma o vulneraciones de derechos de los titulares de los datos[92]. Por su parte, el responsable está en la obligación de elegir a un encargado que ofrezca las máximas garantías de cumplimiento legal, obligación que podía

---

Unión y delegado de protección de datos; los fines del tratamiento; una descripción de las categorías de los interesados y de las categorías de datos personales; categorías de destinatarios, descripción de las medidas de seguridad, etc. (artículo 30 del Reglamento europeo). Este registro deberá presentarse ante la autoridad de control cuando esta así lo requiera . Cabe destacar que la obligación anterior, en principio, no afecta a todos responsables, sino únicamente a aquellos que empleen a 250 personas o más y a aquellos responsables que realicen tratamientos continuados de datos de categorías especiales del artículo 9, datos relativos a condenas o tratamientos especialmente arriesgados para los derechos y libertades. No obstante lo anterior, en nuestra opinión, y dependiendo de la sensibilidad de los datos involucrados en el tratamiento, puede ser aconsejable que el pequeño empresario cree y mantenga actualizado este registro, como mecanismo de transparencia y prueba del cumplimiento de las obligaciones exigidas por el Reglamento ante requerimientos de autoridades competentes o de interesados. Aquellos responsables que deban cumplir la obligación de llevanza del registro de actividad y, por no tener establecimiento en suelo europeo, deban designar a un representante del responsable en la Unión (figura que analizaremos más adelante), realizarán esta tarea de manera conjunta (art. 30.1 del Reglamento europeo).

91 Definición del encargado del tratamiento aportada por el artículo 4.8 del Reglamento General de Protección de Datos: "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

92 El encargado, de acuerdo con la normativa española vigente, tiene las siguientes obligaciones: a) deberá proceder a la llevanza del documento de seguridad cuando así de le haya delegado (art. 88.6 RLOPD); b) debe devolver los datos o ficheros en los que figuren datos personales al responsable, o destruirlos, una vez finalizada la relación contractual (art. 12.3 LOPD y 22.1 RLOPD); y c) debe responder ante el cliente (responsable del tratamiento) en cuanto al cumplimiento de las normas sobre protección de datos y medidas de seguridad acordadas contractualmente, así como por aquellos incumplimientos causados por él o por los subencargados (art. 20.3 y 21.c) RLOPD).

deducirse del marco vigente actual (concretamente, de su sistema de distribución de responsabilidades) y que el nuevo Reglamento europeo ha expresado de forma literal en el primer apartado de su artículo 28[93].

En el ámbito de la computación en la nube, como hemos apuntado en anteriores ocasiones, puede tener lugar una pérdida de control del pequeño empresario, responsable del tratamiento de los datos personales que recabe, sobre aquellos datos que decida realizar procesar, almacenar, etc. mediante servicios de computación en la nube. El proveedor *cloud*, por su parte, al proporcionar las herramientas informáticas y tratando los datos por orden del cliente (almacenándolos en sus servidores, por ejemplo), es considerado legalmente y con carácter general, como encargado del tratamiento, tal y como veremos a continuación.

Como ya hemos señalado respecto de la figura jurídica del responsable, el propio Grupo de Trabajo del Artículo 29 reconoce que existen ciertos criterios que permiten determinar la condición de las distintas partes implicadas (atendiendo, como el mismo Dictamen 1/2010 afirma[94], al nivel de instrucciones dadas por el responsable, al seguimiento que puede realizar el cliente del cumplimiento de sus instrucciones, a los conocimientos especializados de las partes, etc.), y que, en ciertos casos, el proveedor *cloud* pueda considerarse incluso responsable[95] conforme nuestra Ley Orgánica de Protección de Datos (concretamente, como lo recogen los arts. 12.2 y 12.4[96]).

---

93 Artículo 28.1 del Reglamento General de Protección de Datos. "Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado".

94 Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" (WP 169), págs. 31 y 32.

95 Dictamen 5/2012 sobre *Cloud Computing*: "Como se señaló en el dictamen 1/2010, pueden utilizarse algunos criterios para evaluar la responsabilidad del tratamiento. De hecho, pueden darse situaciones en que un proveedor puede considerarse como responsable del tratamiento conjunto o responsable del tratamiento por derecho propio en función de circunstancias concretas. Por ejemplo, este podría ser el caso cuando el proveedor trata datos para sus propios fines".

96 Art. 12.2 y 12.4 LOPD. "2.- La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar. (...). 4. En el caso de que el encargado del tratamiento

En nuestra opinión, el nuevo Reglamento europeo responde a la posibilidad de matizar las responsabilidades del empresario suscriptor de servicios de computación en la nube, al plantear mecanismos complementarios que compensan, al menos en parte, la imposibilidad fáctica de control pleno del tratamiento que realiza el proveedor *cloud*[97]. A la espera de que el nuevo Reglamento Europeo sea aplicable, esperamos que contribuya a conseguir una situación más equitativa (en especial para el profesional o pequeño empresario), al ponerse en práctica mecanismos fiables y acreditados por las instituciones europeas, que permitan aumentar el control del cliente sobre el tratamiento que realiza el proveedor, que le otorguen la máxima transparencia y una capacidad de maniobra al responsable del tratamiento más acordes con la elevada responsabilidad exigida por la normativa vigente y con la naturaleza del concreto servicio *cloud* prestado[98].

De acuerdo con la normativa aplicable actualmente, entre ambos (responsable y encargado del tratamiento) regirá un acuerdo mediante el cual el encargado se comprometa a seguir las instrucciones del responsable en cuanto al tratamiento de los datos personales cedidos, a no destinarlos a finalidades diferentes a las recogidas en el acuerdo, a no comunicarlos a terceros y a implementar las medidas de seguridad técnicas y organizativas que garanticen la seguridad de los datos de carácter personal (12.2 LOPD[99]).

---

destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".

97 Nos sumamos a la opinión de RUBÍ NAVARRETE, cuando propone que las fórmulas alternativas sean jurídicamente vinculantes, permitan a las autoridades de control ejercer sus competencias, y que incorporen opciones que permitan a los titulares de los datos ejercer sus derechos y obtener compensaciones en caso de vulnerarse sus garantías. RUBÍ NAVARRETE, Jesús, *op. cit.,* pág. 101.

98 Sería recomendable, además de lo anterior, y según nuestra opinión, que se introdujera una información más transparente en los contratos *cloud*, por ejemplo, sobre los potenciales subencargados, proveedores externos y socios comerciales (sugerimos la exigencia de publicación en el sitio web del proveedor de las identidades, así como posibilitar al responsable la rescisión del contrato), o el detalle de aquellas localizaciones de datos o finalidades del tratamiento que suelen venir enunciadas de forma genérica, bajo expresiones del tipo "para proporcionar y mejorar nuestros servicios", "peticiones gubernamentales", etc. Habrá que atender a cómo los proveedores de computación en la nube se adaptan al nuevo Reglamento europeo.

99 Artículo 12.2 LOPD. "La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".

El nuevo Reglamento europeo es más específico y estricto en relación con este contrato entre responsable y encargado del tratamiento. Establece que el acuerdo entre ambos deberá detallar el objeto, duración, naturaleza y finalidad del tratamiento, los tipos de datos personales y categorías de interesados[100] y los derechos y obligaciones del responsable. Asimismo, mediante este documento, el encargado del tratamiento se obligará a garantizar la confidencialidad de esos datos y a adoptar las medidas técnicas y organizativas de seguridad de los datos, recabará autorización del responsable en cuanto a subencargados, ayudará al responsable a demostrar el cumplimiento de lo acordado y exigido legalmente, y, una vez finalice la prestación de servicios, se obligará a suprimir o devolver los datos (a elección del responsable) y a eliminar las copias que puedan quedar remanentes, excepto que deban conservarse por obligación legal (art. 28.3 del Reglamento europeo[101]).

Por otra parte, en la prestación de servicios de computación en la nube sucede que el proveedor que oferta los servicios al pequeño empresario responsable del tratamiento es quien decide los territorios en los que se producirá y qué entidades colaborarán en el tratamiento de los datos (por ejemplo, subcontratas del propio proveedor *cloud*), así como las medidas de seguridad y demás protocolos internos que protegerán los datos migrados. Aunque a menudo existirá una previsión contractual mínima, la realidad es que no se suelen dar al cliente opciones de negociación de cláusulas ni mecanismos adicionales que permitan controlar el

100 El Reglamento General de Protección de Datos no especifica en qué consiste esta categorización de interesados. Habremos de estar a las posibles interpretaciones que realicen de este término las autoridades nacionales de control.

101 Artículo 28.3 del Reglamento General de Protección de Datos. "El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado: a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento(...); b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad (...); c) tomará todas las medidas necesarias de conformidad con el artículo 32; d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento; e) asistirá al responsable, (...); f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, (...); g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros; h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, (...)".

cumplimiento de sus instrucciones.

El Grupo de Trabajo del Artículo 29 es consciente de este escaso margen de maniobra que a menudo padece el empresario suscriptor de servicios *cloud* en el marco de la negociación de contratos tipo (tan extendidos en la contratación *online*), entre cuyas cláusulas predispuestas se hallará el contrato entre responsable y encargado del tratamiento, contrato exigido por la normativa en materia de protección de datos, como se ha mencionado. Sin embargo, es el cliente (a menudo pequeño empresario), quien decide que todo o parte del tratamiento se desarrolle en entornos *cloud*, y por ello, como se ha visto, le corresponde el papel de responsable del tratamiento. Por su parte, el proveedor *cloud* (quien generalmente es una gran empresa que pone a disposición del cliente las cláusulas contractuales para su suscripción) debería, a tenor de lo establecido legalmente, seguir las instrucciones del responsable en todo momento, es decir, del pequeño empresario, respecto del tratamiento de datos personales.

Bajo nuestro punto de vista, la clave de la aplicación práctica de la normativa actual es precisamente este desequilibrio contractual existente entre las partes, que puede mermar la protección otorgada por la normativa a los titulares de datos personales o conllevar potenciales "conflictos negativos de competencia[102]" que pueden suponer un incumplimiento de las obligaciones impuestas por la Directiva y por sus transposiciones nacionales.

Tengamos en cuenta, una vez más, que es el responsable quien "deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento" (art. 20.2 RLOPD), independientemente de las condiciones predispuestas por el proveedor *cloud* con quien decida contratar[103]. Por ello, consideramos loables las mayores exigencias del Reglamento europeo a la persona del encargado y al contrato entre ambos, así como el resto de mecanismos (códigos de conducta, medios de certificación, sellos, etc.) y figuras (delegado del

102 Es decir, que ni el proveedor (encargado del tratamiento) ni la empresa (responsable del tratamiento) asuman la responsabilidad en ciertos casos, debido a lagunas de la normativa. Esta misma expresión es la que recoge el Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" (WP 169), pág. 25.

103 Así lo afirma el el GT29 en su Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento" (WP 169): "el desequilibrio en la capacidad de negociación entre un pequeño responsable respecto de los grandes proveedores no puede servir de justificación al responsable para que acepte cláusulas contractuales que no cumplan los requisitos legales de protección de datos". (Traducción propia).

tratamiento, responsable en la Unión, dación de mayores competencias a las autoridades de control) que auxiliarán al responsable en el cumplimiento del marco legal y al interesado en el ejercicio práctico de sus derechos y en el aporte de las máximas garantías respecto de sus datos personales.

Con todo, el pequeño empresario deberá sopesar, además de su importante responsabilidad en materia de protección de datos y de elección adecuada del proveedor, sus posibilidades económicas en cuanto a la adopción de estas garantías, ya que, por ejemplo, la obtención de sellos de calidad, certificaciones, contratación de un delegado de protección de datos, etc. suelen suponer un coste económico elevado para el pequeño empresario.

Además, con carácter general, el encargado del tratamiento (en nuestro caso, el proveedor de servicios de computación en la nube) será considerado como responsable a efectos sancionadores cuando se exceda del mandato del responsable y determine otras finalidades del tratamiento, no cumpla con las instrucciones del responsable o filtre datos o incumpla el acuerdo suscrito entre ambos sobre el tratamiento (arts. 12.4 LOPD, 20.3 RLOPD y 28.10 del Reglamento General de Protección de Datos).

Por otra parte, como señalan algunos autores con quienes coincidimos, dentro del deber de diligencia exigible al proveedor *cloud* como encargado del tratamiento se encuentra informar al responsable de forma detallada sobre: a) la tipología de nube, servicios, participantes, etc.; b) las medidas de seguridad (niveles de seguridad, auditoría, encriptación, incidencias de seguridad, etc.); y c) la portabilidad al término del contrato[104].

Tanto el proveedor *cloud* (como encargado del tratamiento) como el cliente de servicios *cloud* (en su calidad de responsable), así como cualesquiera subencargados que actúen bajo su mandato, tienen el deber de guardar confidencialidad en relación a cualesquiera datos personales de los que hayan tenido conocimiento por razón del desempeño de su tratamiento[105]. Este deber de secreto debería subsistir, a nuestro parecer, incluso finalizadas las relaciones con el

104 FERNÁNDEZ ALLER; Cecilia, "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (Cloud Computing)", *Revista de Derecho UNED*, núm. 10, 2012, págs. 125 a 145.

105 Deber de confidencialidad del responsable, del encargado y de los subencargados: art. 10 de la LOPD y art. 16 de la Directiva 95/46/CE.

responsable del tratamiento (o, en su caso, con el titular de los datos personales)[106].

Como recomendaron ya algunos autores en su momento[107], el proveedor de servicios *cloud* debería considerar, en el diseño de su oferta de servicios, la elección de un procedimiento que cumpla con los estándares técnicos en materia de protección de datos; estándares que satisfagan los requisitos de seguridad y privacidad de los clientes de mayor riesgo, así como considerar la incorporación de un esquema sólido de controles desde un inicio, para asegurar que se cumpla con los requerimientos de la mayoría de clientes y disminuyendo la necesidad de personalizar soluciones[108]. También, que el proveedor definiese desde la arquitectura del servicio tanto los controles implementados por defecto como aquellos que deban o puedan ser definidos por el usuario, así como las políticas, procedimientos y procesos asociados con los requerimientos de privacidad, que deben ir revisándose y actualizándose de acuerdo a las exigencias de los clientes. En nuestra opinión, estos mecanismos pueden establecerse a modo de protección de datos desde el diseño, cuyos principios se definen en el artículo 25 del Reglamento europeo.

3.3.4.- El subencargado del tratamiento

Como sabemos, la prestación de servicios de computación en la nube puede

106 Ver apartado "La confidencialidad de los datos del cliente y las solicitudes de acceso a terceros", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

107 GARCÍA SÁNCHEZ, Manuel, *op. cit.,* pág. 51.

108 Por ejemplo, el estándar de seguridad y privacidad en *Cloud Computing* ISO/IEC 27018, en línea con la normativa europea en materia de protección de datos. En opinión de COTINO, respecto de la regulación en materia de computación en la nube, "la gobernación vertical y la heterorregulación por los poderes públicos queda en general obsoleta", y "la regulación que pretenda tener alguna eficacia debe ser el resultado de fórmulas de gobernanza en las que participe activamente el sector afectado sobre el que tienen que aplicarse las normas", con lo cual aboga por regulaciones "más suaves" que provengan de "la participación de la comunidad afectada (instituciones, individuos y las entidades empresariales implicadas)", y considera que "tal regulación tiene necesariamente que ser aceptada y hacerse propia por los Estados e instituciones, que tienen que hacer valer tales normas". Esta regulación, que el autor califica como "nebulosa", se manifiesta en actuaciones declarativas (guías, recomendaciones, buenas prácticas, etc.) de las autoridades en materia de protección de datos, y en regulaciones técnicas por parte del sector *cloud*. Estas normas de *soft law* serán la inspiración de futuras normas vinculantes adoptadas por el legislador europeo y estatal, y por el momento, cumplen la misión de "colmar las lagunas e incertidumbres de una normativa no concebida para la nube". COTINO HUESO, Lorenzo, "Algunas cuestiones clave de protección de datos en la nube. Hacia una regulación nebulosa", *Revista catalana de dret públic*, núm. 51, 2015, pág. 93. Sobre las mismas cuestiones, MARZO PORTERA, Ana Maria; "Privacidad y Cloud Computing: Hacia dónde camina Europa", *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche*, Vol. 1, núm. 8, 2012, págs. 202 a 229.

involucrar a múltiples proveedores (de hardware, de almacenamiento, de comunicaciones, etc.) con acceso a datos personales, que actuarán como subencargados[109]. De forma general, la subcontratación está perfectamente permitida por la Directiva 95/46/CE[110], y en la regulación del art. 21 del RLOPD[111]. En esta normativa se observa la exigencia general de conocimiento de la identidad de las empresas subcontratistas y de autorización previa del responsable del tratamiento, en cuyo nombre se efectuará la subcontratación.

No obstante, el segundo apartado del artículo 21 excepciona la exigencia general de autorización del responsable al cumplimiento de cuatro requisitos acumulativos, siempre previos a la perfección de la subcontratación y que, si bien eximen de la autorización del responsable del tratamiento, no eximen al encargado del tratamiento de comunicarle al responsable el tipo de servicio subcontratado, las características o identidad de los posibles subcontratistas y las garantías que ofrecen

---

109 En los contratos de computación en la nube, en ocasiones se les menciona como *partners* o "socios comerciales", aunque de acuerdo con la normativa sobre protección de datos, corresponden a la figura jurídica de subencargados del tratamiento, tal y como reconoce la "Guía para clientes que contraten servicios de Cloud Computing", publicada por la AEPD. Estos subproveedores pueden ser parte de una larga cadena de subcontrataciones, entre cuyos operadores se transmiten datos personales migrados por el cliente-responsable. AEPD, *Guía para clientes que contraten servicios de Cloud Computing,* [en línea]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf>. [Fecha de consulta: 12 de mayo de 2017].

110 El Grupo de Trabajo del Artículo 29, en su Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", afirma que "No hay nada en la Directiva que impida que, por exigencias organizativas, se pueda designar a varias entidades como encargadas (o subencargadas) del tratamiento de datos, incluso subdividiendo los cometidos en cuestión. Ahora bien, todas ellas tienen que ajustarse a las instrucciones dadas por el responsable del tratamiento de los datos al llevar a cabo el tratamiento". GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento"...*, *op. cit,* pág. 30.

111 Art. 21 Real Decreto 1720/2007, que aprueba el RLOPD: "El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento. 2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos: a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar. Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación. b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero. c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior. En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento. 3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior".

al proveedor con quien contratan parte del servicio. Entre estos requisitos del artículo 21.2 del RLOPD se encuentra la necesidad de comunicar al responsable la identidad de los contratistas (art. 21.2.a, segundo inciso), así como la firma de un contrato entre el encargado del tratamiento y subcontratista conforme a lo establecido por el artículo 20, y adquiriendo el subcontratista, de este modo, la calificación de encargado del tratamiento, y debiendo cumplir con las obligaciones que ello conlleva. El apartado tercero del artículo 21 del RLOPD deja las puertas abiertas a la subcontratación parcial de la prestación del servicio de manera posterior a la celebración del contrato entre responsable y encargado, siempre que se cumplan los mismos requisitos que exigía el apartado anterior.

El Grupo de Trabajo, en su Dictamen 5/2012 sobre la computación en la nube, reconoce que es habitual la múltiple subcontratación entre proveedores y subproveedores *cloud*, y la considera como un riesgo para la protección de datos[112]. Asimismo, considera que "En tales supuestos, las obligaciones y responsabilidades derivadas de la legislación sobre protección de datos deberán consignarse claramente y no dispersarse a lo largo de la cadena de externalización o subcontratación, con el fin de garantizar el control efectivo sobre las actividades de tratamiento y asignar una responsabilidad clara a este respecto"[113]. A nuestro parecer, lo idóneo sería que estos mecanismos de información no entorpeciesen la naturaleza dinámica de la prestación del servicio *cloud*, que puede implicar subcontrataciones a medida que el desarrollo empresarial así lo requiera[114].

---

112 Afirma el Grupo de Trabajo del Artículo 29 en su informe que "La mayoría de estos riesgos se dividen en dos grandes categorías, a saber, la falta de control de los datos y la insuficiente información sobre la propia operación de tratamiento (falta de transparencia)". Respecto de la pérdida de control sobre los datos, reconoce que existe la "Falta de posibilidad de intervención debido a la complejidad y la dinámica de la cadena de subcontratación: el servicio de computación en nube ofrecido por un proveedor puede realizarse combinando servicios de varios proveedores distintos, que pueden añadirse o suprimirse dinámicamente a lo largo de la duración del contrato del cliente". Respecto de la falta de transparencia en la información facilitada por el proveedor, el Grupo de Trabajo reconoce que "Algunas posibles amenazas pueden derivarse de que el responsable del tratamiento no sepa que: Se realiza un tratamiento en cadena con múltiples encargados del tratamiento y subcontratistas". GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 5/2012 sobre Cloud Computing, op. cit.*, págs. 6, 7.

113 GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 5/2012 sobre Cloud Computing, op. cit.*, pág. 11.

114 Llegados a este punto, quizás debería plantearse al proveedor una distinción entre subcontratas que impliquen tratamiento de datos personales o su cambio de localización (en cuyo caso deberían demostrar su cumplimiento con los requisitos legales europeos en materia de protección de datos); y subcontratas meramente técnicas o que no supongan migraciones o potenciales accesos a datos personales, tal y como propuso el Grupo de Expertos de la *Cloud Computing Strategy*. *Cloud Computing Strategy*, *Discussion Paper on Subcontracting,* [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/files/expert_groups/expert_group_subcontracting_discussion

La práctica demuestra que consumidores y pequeñas empresas a menudo no están al corriente ni de las cadenas de contratos que sustentan la prestación de un determinado servicio ni de las obligaciones correspondientes a cada uno de los integrantes de esta cadena[115]. Así, por ejemplo, los integradores no operan directamente, sino que gestionan subcontratos; los centros de datos, claves para la prestación de servicios *cloud*, generalmente están dirigidos por subcontratistas y no por el proveedor principal del servicio, etc.

Consecuentemente, los subproveedores a menudo ostentan mayor fuerza contractual que el proveedor principal, que es quien contrata con el cliente-responsable, con lo cual puede suceder que el proveedor principal ofrezca al cliente unas condiciones, en cuanto a protección de datos y medidas de seguridad, más garantistas de las que él mismo tiene con su subproveedor. Si el contrato con el cliente es posterior a la subcontrata, ya no existe posibilidad de renegociación para incluir la peticiones de los clientes[116]. Al respecto, consideramos que el proveedor *cloud*, al actuar como encargado del tratamiento, deberá cambiar de subcontratista cuando tenga conocimiento de que se incumplen las garantías acordadas con el

---

_paper_en.pdf>. [Fecha de consulta: 12 de mayo de 2017].

115 La práctica nos demuestra que, si bien muchos proveedores manifiestan la posibilidad de que terceros proveedores puedan acceder a nuestros datos, la identidad de estos queda oculta o difuminada bajo una categoría general (nuestros socios, nuestros proveedores...). A modo de ejemplo, esta cláusula que informa sobre subcontratación, de la política de privacidad del software como servicio *Dropbox para empresas*: "Podríamos compartir información tal y como se describe en las siguientes secciones, pero no la venderemos a terceros con fines publicitarios ni de ningún otro tipo. (...). Dropbox confía en ciertos proveedores externos (por ejemplo, proveedores de servicios de asistencia al cliente e informática) que nos ayudan a proporcionar, mejorar, promocionar y proteger nuestros servicios. Estos proveedores podrán acceder a tu información exclusivamente para realizar tareas en nuestro nombre y de forma acorde con esta Política de privacidad, y seremos los únicos responsables de su gestión de tu información de acuerdo con nuestras instrucciones". Aunque, por ejemplo, Dropbox admite que un tercer proveedor proporciona los servidores de almacenamiento en Estados Unidos, en ningún momento menciona que sus servicios están soportados sobre la infraestructura de "Amazon S3" para ofrecer su almacenamiento elástico y escalable, pese a que sus relaciones con este subproveedor están consolidadas desde hace años. De todos modos, en cumplimiento de la LOPD y de su reglamento de desarrollo, no puede negarse a facilitar una información más detallada sobre las identidades o garantías en caso de que el cliente-responsable le solicite más información sobre las subcontrataciones que impliquen la transferencia de datos, más aun si suponen localizaciones en terceros países sin nivel adecuado de protección. Información disponible en: <https://www.dropbox.com/es_ES/privacy#privacy>, <https://www.dropbox.com/help/7> y <http://www.datacenterknowledge.com/archives/2013/10/23/how-dropbox-stores-stuff-for-200-million-users/>. [Fecha de consulta: 12 de mayo de 2017]. Esta falta de transparencia también se recoge por la *Cloud Computing Strategy*, en su *Discussion Paper on Subcontracting* (pág. 3).

116 *Cloud Computing Strategy*. *Discussion paper on Subcontracting*, *op. cit.*, síntesis anexa, de fecha 27 y 28 de marzo.

responsable. Puesto que se ha comprometido contractualmente con el responsable en cuanto a la prestación de las garantías legalmente exigibles, en caso de que incumpla tales estipulaciones será considerado responsable a efectos sancionadores (art. 12.4 LOPD[117]).

La "Guía para prestadores de servicios de *Cloud Computing"*, publicada por la Agencia Española de Protección de Datos[118], reconoce que formará parte del deber de diligencia del proveedor de servicios de computación en la nube proporcionar una información transparente al responsable, especialmente de aquellos mecanismos que permitan cumplir con las exigencias legales. Para suplir estas carencias que tienen lugar en la práctica, sin embargo, deberá ser el responsable quien solicite del proveedor *cloud* la información sobre subcontrataciones que considere necesaria, para asegurarse el cumplimiento de la normativa española sobre protección de datos, y así poder elegir aquel proveedor que mayores garantías le ofrezca en cuanto al cumplimiento de la normativa vigente[119].

Para mantener el control en el tratamiento a través de las diferentes subcontrataciones, el Grupo de Trabajo del Artículo 29 recomienda el uso de garantías similares a las propuestas por la Comisión, en su Decisión de 5 de febrero de 2010, para la transferencia de datos personales a encargados del tratamiento establecidos en terceros países[120]. En estas cláusulas tipo únicamente se permite la subcontratación con autorización previa y por escrito del responsable del tratamiento, y con la existencia de un acuerdo que imponga al subencargado las mismas obligaciones que tiene encargado del tratamiento. En caso de que el subencargado incumpla con sus obligaciones, será el encargado quien responda ante el responsable. Aunque el Grupo de Trabajo no lo mencione, puesto que su

117 Art. 12.4 LOPD. "En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente".

118 *Guía para prestadores de servicios de Cloud Computing* [en línea]. Disponible en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf>. [Fecha de consulta: 12 de mayo de 2017].

119 La "Guía para clientes que contraten servicios de Cloud Computing", publicada por la AEPD, recoge un abanico de preguntas a las cuales es altamente recomendable que la empresa que pretenda suscribir este tipo de servicios dé respuesta antes de proceder a contrataciones que impliquen tráfico de datos personales [en línea]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf>. [Fecha de consulta: 25 de agosto de 2016].

120 GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 5/2012 sobre Cloud Computing, op. cit.*, pág. 11.

aprobación fue posterior a la redacción del Dictamen 5/2012 sobre *Cloud Computing*, consideramos igualmente recomendables las cláusulas tipo entre encargado establecido en el EEE y subencargado establecido fuera del EEE, adoptadas por la AEPD en su resolución de transferencia internacional de datos de 16 de octubre de 2012[121].

Además, la realidad transfronteriza de muchas de estas subcontrataciones maximiza la problemática de la pérdida de control sobre los subcontratistas, tal y como hemos observado en cuanto a su identificación, lugar de establecimiento y efectiva implementación de las medidas de seguridad técnicas y organizativas acordadas, si no se sigue un estricto protocolo de actuación[122]. En especial, cuando estas subcontrataciones impliquen la transferencia de datos a terceros países cuya protección no se considere adecuada, deberá cumplirse con los requisitos para la transferencia internacional legal de datos personales (cuya regulación actual se halla en el Título VI del RLOPD), entre los cuales se encuentra la necesidad de incluir mecanismos que permitan garantizar la preservación del nivel de protección, como la incorporación de cláusulas tipo de encargado a subencargado[123].

Además de la identificación de los servicios y de la empresa subcontratante, incluyendo el país en el cual esta empresa aloja los datos, y la posibilidad de alternativas para el cliente en caso de que esté de acuerdo con esta subcontratación (por ejemplo, la rescisión del contrato sin penalizaciones), la LOPD exige que, cuando intervengan empresas subcontratadas, debe celebrarse un contrato entre el encargado del tratamiento y el subcontratista que incluya garantías equivalentes a las incluidas en el contrato entre el encargado del tratamiento y el responsable, de

121 Estas cláusulas se estudiarán con más detalle en el apartado dedicado a las transferencias internacionales de datos, en este mismo capítulo. Se trata del modelo de cláusulas contractuales de la AEPD para encargado establecido en España y subencargado de tercer país sin nivel adecuado de protección, basadas en el Considerando 23 de la Decisión 2010/87/UE, que permite a las autoridades nacionales flexibilizar la subcontratación entre encargados nacionales y subencargados de países sin nivel de protección adecuado [en línea]. Disponible en: <https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/common/pdfs/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf>. [Fecha de consulta: 12 de mayo de 2017].

122 MARZO PORTERA, Ana María; "Privacidad y Cloud Computing, hacia dónde camina Europa", *Revista de la Facultad de Ciencias Sociales y Jurídicas de Elche,* vol. I, núm. 8, 2012, págs. 202-229.

123 Ver apartado "Transferencias internacionales de datos y *Cloud Computing"*, en este mismo capítulo.

acuerdo con lo establecido por los mencionados art. 12 LOPD y art. 21 RLOPD[124]. El Grupo de Trabajo del Artículo 29, en el mencionado Dictamen 5/2012 establece los contenidos que deberá especificar el contrato entre el proveedor de computación en la nube y el empresario que los suscriba respecto de las subcontrataciones[125].

Igualmente, nos sumamos a la recomendación de ciertos autores de someter la subcontratación en los servicios de computación en la nube a otros requisitos añadidos, como por ejemplo que se previera la gestión de incidentes de seguridad acontecidos entre encargado y subcontratistas, y la expresa asunción y delimitación de todas las obligaciones relevantes en materia de tratamiento de datos personales[126].

Como se verá en posteriores apartados, dado que el pequeño empresario responsable del tratamiento deberá asegurarse de que el proveedor *cloud* garantice una supresión segura de los datos y que el contrato entre el proveedor y el cliente contenga disposiciones claras relativas a la supresión de los datos personales, lo mismo se aplica a los contratos entre proveedores y subcontratistas. Según el Grupo de Trabajo del Artículo 29, "la supresión de datos es pertinente tanto a lo largo de la duración de un contrato de computación en nube como a su finalización", y también "es pertinente en caso de sustitución o retirada de un subcontratista".

En resumen, el Grupo de Trabajo del Artículo 29 permite al encargado del tratamiento (es decir, al proveedor *cloud*) subcontratar sus actividades cuando

---

124 Apartados primero y segundo del art. 12 LOPD. "No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. 2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".

125 "El contrato deberá especificar que sólo podrá contratarse subencargados del tratamiento previa autorización que puede otorgar en general el responsable del tratamiento, en consonancia con la inequívoca obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de cualquier cambio previsto a este respecto, teniendo el responsable del tratamiento en todo momento la posibilidad de oponerse a tales alteraciones o de rescindir el contrato. Deberá existir una clara obligación para el proveedor de nombrar a todos los subcontratistas contratados (por ejemplo, en un registro digital público). Deberá garantizarse que los contratos suscritos entre proveedores y subcontratistas reflejen las condiciones del contrato entre el cliente y el proveedor (esto es, que los subencargados del tratamiento están sujetos a los mismos derechos contractuales que el proveedor). En particular, deberá garantizarse que tanto el proveedor como todos los subcontratistas sólo actuarán siguiendo instrucciones del cliente. Tal como se explica en el capítulo sobre el subtratamiento, la cadena de responsabilidad deberá exponerse claramente en el contrato. Deberá fijarse la obligación por parte del encargado del tratamiento de definir las transferencias internacionales, por ejemplo firmando contratos con subcontratistas, basándose en las cláusulas contractuales tipo 2010/87/UE". Grupo de Trabajo del Art. 29, Dictamen 1/2012 sobre *Cloud Computing*, pág. 15.

126 PUYOL MONTERO, Javier; *Algunas consideraciones..., op. cit.*, págs. 103 a 104.

cuente con el consentimiento del responsable del tratamiento. Este consentimiento podrá recabarse al inicio del servicio, respecto de las subcontratas existentes en el momento de suscribirse en contrato entre responsable del tratamiento y encargado. Sin embargo, si durante el transcurso de la prestación se producen cambios en las subcontrataciones o en las identidades de los subcontratistas que puedan afectar a las garantías en materia de protección de datos, el responsable del tratamiento debe ser informado de tales cambios y poder optar a rescindir el contrato en caso de disconformidad[127]. Asimismo, el Grupo de Trabajo del Artículo 29 considera necesario que entre encargado y subencargado se firme un contrato que permita garantizar las disposiciones en materia de protección de datos acordadas entre responsable y encargado. Ello es así porque el cliente, como responsable del tratamiento, solo puede valorar la capacidad de cumplimiento de las obligaciones legales del proveedor *cloud* y sus subcontratistas si es informado de manera adecuada sobre las condiciones en que se efectúa la prestación y las identidades de quienes lo realizan[128].

Por último, el Grupo de Trabajo del Artículo 29 considera que el responsable debe poder interponer acciones ante incumplimientos del subencargado, ya sea a través de responsabilidad directa del encargado por incumplimientos de cualesquiera de sus subcontratantes, ya sea porque así se disponga en el contrato entre encargado

127 En el mismo sentido, e interpretando el artículo 21.2.a) del RLOPD, el fundamento jurídico décimo de la Sentencia del Tribunal Supremo 1720/2007, de 15 de julio de 2010, establece que "Si conforme a dicho artículo [en referencia al art. 3. d) de la LOPD] el responsable del fichero o tratamiento es la persona física o jurídica, de naturaleza pública o privada, u organismo administrativo, que decide sobre la finalidad, contenido y uso del tratamiento, es del todo lógico y está implícito en la norma legal de mención que el encargado del tratamiento comunique al responsable la necesidad de subcontratar y con quién pretende hacerlo, máxime cuando el responsable del tratamiento debe velar, como expresa el artículo 20.2 del Reglamento, (...), para que el encargado del tratamiento reúna las garantías para el cumplimiento de lo en él dispuesto. Dicho lo anterior es obligado indicar, contrariamente a lo que sostiene el Abogado del Estado, que aunque el artículo 21 no contiene una previsión específica sobre la facultad del responsable del tratamiento en orden a la comunicación de subcontratación, es claro que esa comunicación del encargado del tratamiento constituye en realidad una propuesta que puede ser rechazada por aquel, bien por entender improcedente la subcontratación, bien por considerar inidónea la empresa con la que se pretende subcontratar. Así se infiere de la capacidad de decisión del responsable del tratamiento y de la responsabilidad que le corresponde. Si el responsable del tratamiento, de conformidad con el artículo 17.2 de la Directiva, debe elegir un encargado del tratamiento que ofrezca garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deben efectuarse, y asegurarse que se cumplen dichas medidas, y si de conformidad con el apartado 3 del indicado artículo el encargado del tratamiento solo actúa siguiendo instrucciones del responsable del tratamiento, negar capacidad de disposición a éste en supuestos de subcontratación es una conclusión reñida con los más elementales criterios de la lógica ".

128 "La transparencia en la nube supone que es necesario que el cliente tenga conocimiento de todos los subcontratistas que contribuyan a la prestación de los respectivos servicios en nube, así como de la localización de todos los centros donde puedan tratarse los datos personales". GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 5/2012 sobre Cloud Computing, op. cit.*, pág. 13.

y subencargado del tratamiento[129].

El nuevo Reglamento europeo (apartados 2 y 4 del art. 28) recoge igualmente la posibilidad de que el encargado delegue todo o parte del tratamiento a otro encargado (en este caso, la norma no se refiere al término "subencargado"), con autorización escrita general o específica, a quien se le exigirán las mismas garantías que ofrece el primero al responsable del tratamiento[130]. Consideramos que el Reglamento europeo ha introducido una mejora destacable respecto de la anterior normativa, puesto que, efectivamente, no permite la subcontratación del tratamiento de datos personales sin autorización previa y por escrito, del responsable. Según el propio artículo 28.2 del Reglamento europeo, esta autorización puede ser general o específica, con lo cual deberemos estar a posibles adaptaciones de nuestra normativa nacional al RLOPD para saber si se exigirá que el responsable conozca la identidad de los subcontratistas o si será suficiente, como permite la redacción del Reglamento, con un consentimiento general sobre subcontrataciones, siempre que estas presten las suficientes garantías en cuanto a medidas técnicas y organizativas, y cumplan con sus correspondientes obligaciones en materia de protección de datos, tal y como exige el mismo Reglamento europeo en su artículo 28.4.

Otra mejora importante respecto de la normativa actual es que el nuevo Reglamento obliga expresamente a informar al responsable de cualquier cambio en la cadena de subencargados, permitiéndole oponerse en caso de no estar de acuerdo (art. 28.2). Aunque el Reglamento no lo manifieste expresamente, deducimos que esta obligación del encargado de informar al responsable sobre los cambios en las subcontataciones una vez suscrito el contrato de prestación de servicios responde al objetivo de que el responsable disponga de esta información permanentemente

129 GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 5/2012 sobre Cloud Computing, op. cit.*, pág. 11.

130 Artículo 28 del Reglamento General de Protección de Datos, apartados 2 y 4. "2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios. (...) 4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado".

actualizada.

Si es así, podría entenderse que el cliente *cloud* responsable del tratamiento debería conocer de antemano la identidad de los subproveedores de servicios de computación en la nube que prestan servicios al proveedor principal y por ello tienen acceso a datos personales migrados por el cliente, y con qué finalidades pueden tratar esos datos, para decidir de manera informada sobre la oportunidad o no de suscribir el contrato de servicios con el proveedor *cloud* o, en su caso, de rescindirlo.

A nuestro parecer, si bien la transparencia en cuanto a aspectos de la subcontratación resulta un aspecto verdaderamente importante para el pequeño empresario que suscriba servicios de computación en la nube para tratar datos personales, sería suficiente con el compromiso del proveedor *cloud* (encargado del tratamiento) de que el subencargado elegido aporta las suficientes garantías en materia de protección de datos, tal y como exige, mediante acuerdo, el artículo 28.4. Ello es así porque el último inciso del artículo 28.4 establece que será el encargado del tratamiento (en nuestro caso, el proveedor *cloud* principal) quien será plenamente responsable ante el pequeño empresario suscriptor (responsable del tratamiento) en caso de que el subencargado (es decir, el proveedor subcontratado) incumpla sus obligaciones en materia de protección de datos[131].

3.3.5.- Las nuevas figuras que incorpora el Reglamento Europeo de Protección de datos: el delegado de protección de datos y el representante del tratamiento en la Unión

El delegado de protección de datos, conocido también como *Data Protection Officer* o DPO, es una figura nueva que nace del Reglamento General de Protección de Datos. Aparece regulado en sus artículos 37 a 39, y juega su papel de forma conjunta con el responsable y al encargado. Según el artículo 67.5 del Reglamento, el delegado de protección de datos "será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39".

Sus funciones se recogen en el artículo 39, y consisten en el asesoramiento al

131 Último inciso del art. 28.4 del Reglamento General de Protección de Datos: "Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado".

responsable y encargado, así como al resto de empleados de la organización, en cuestiones relacionadas con sus obligaciones en materia de protección de datos (entre ellas, la evaluación de impacto) y en el contenido de las disposiciones del marco legal de privacidad. Supervisarán el cumplimiento de la normativa, y se encargarán de la adopción de políticas adecuadas al respecto, así como de asignar responsabilidades, formar a la plantilla, etc. Además, ejercerá de punto de contacto del interesado en cuanto al tratamiento de sus datos personales y al ejercicio de sus derechos (art. 38.4[132]) y deberá colaborar con la autoridad de control cuando esta así se lo requiera (art. 39 del Reglamento[133]). Asimismo, el delegado de protección de datos estará sometido al deber de confidencialidad o secreto profesional (arts. 37.5 y 38.5[134]). El Grupo de Trabajo del Artículo 29, por su parte, ha elaborado las Directrices sobre los delegados de protección de datos, en las que aclara cuándo debe entenderse como obligatorio su nombramiento, qué tareas debe desempeñar y cuáles son los recursos con los cuales es recomendable que cuente, entre otras cuestiones[135].

Debe designarse por el responsable y el encargado en aquellos casos en los

132 Artículo 38.4 del Reglamento General de Protección de Datos. "4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento".

133 Artículo 39 del Reglamento General de Protección de Datos. "El delegado de protección de datos tendrá como mínimo las siguientes funciones: a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros; b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35; d) cooperar con la autoridad de control; e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto. 2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento".

134 Artículo 37.5 del Reglamento General de Protección de Datos. "5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39". Artículo 38.5 del Reglamento General de Protección de Datos. "5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros".

135 Para más detalle sobre esta figura, nos remitimos al documento del Grupo de Trabajo del Artículo 29 *Directrices sobre los delegados de protección de datos* (GT 243) [en línea]. Disponible en:
<http://www.agpd.es/portalwebAGPD/internacional/textosynormas/textos_union_europea/textos_articulo_29/common/es_es_wp243_en_40855_DPO.PDF>. [Fecha de consulta: 6 de junio de 2017].

que el tratamiento se lleve a cabo por una autoridad u organismo público (excepto tribunales cuando lleven a cabo su función judicial); o cuando se realicen tratamientos de datos que requieran observaciones sistemáticas de interesados a gran escala; o tratamientos a gran escala de datos especialmente sensibles de acuerdo con las categorías de los artículos 9 y 10 del mismo Reglamento europeo, de acuerdo con el artículo 37.1 del Reglamento. En otros casos, su nombramiento será facultativo, a no ser que resulte obligatorio de la aplicación de otras normas nacionales complementarias (art. 37.4 del Reglamento europeo). Su identidad se publicará y se comunicará a la autoridad de control (art. 37.7 del Reglamento europeo)

La relación con el responsable y el encargado de tratamiento respectivos que lo nombren puede sustentarse en un contrato laboral o de arrendamiento de servicios. Sin embargo, el desempeño de sus funciones será independiente, debiendo ser asistido por el responsable y el encargado para el desempeño de sus funciones y el mantenimiento actualizado de sus conocimientos, y si poder ser destituido o sancionado por el desempeño de labores derivadas de su cargo, debiendo rendir cuentas únicamente a los máximos responsables de la organización empresarial o institución (apartados 2 y 3 del artículo 38[136]).

El artículo parece ideado para entidades de considerable envergadura y masivo manejo de datos, entre las cuales se encontrarán muchos proveedores de servicios de computación en la nube. En cuanto a la obligatoriedad de su nombramiento por parte de pequeños empresarios, siempre y cuando su actividad principal no sea el tratamiento masivo de datos personales, no parecen estar obligados a designar un delegado de protección de datos. Sin embargo, creemos que es conveniente que su designación, especialmente para aquellas pequeñas empresas que traten datos de categorías especialmente sensibles de acuerdo con los artículos 9 y 10 del Reglamento europeo, hasta que se interprete por las autoridades y tribunales competentes el concepto jurídico indeterminado de "tratamiento de datos a gran escala", no definido por la propia norma.

136 Artículos 38.2 y 38.3 del Reglamento General de Protección de Datos. "2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados. 3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado".

Otra figura introducida por el Reglamento General de Protección de Datos es el denominado representante del responsable o del encargado del tratamiento, definido en su artículo 4.17[137] y regulado en su artículo 27[138]. Según el nuevo Reglamento, cuando el responsable (o encargado del tratamiento) no esté establecido en la Unión Europea, pero realice actividades relacionadas con la oferta de bienes o servicios a los ciudadanos de la Unión (por ejemplo, un proveedor *cloud* establecido en EE. UU.) o se vigile el comportamiento de interesados europeos dentro de la Unión (art. 3.2), este designará por escrito a un "representante del responsable" (o "representante del encargado", en su caso), excepto que se trate de un tratamiento ocasional o de un organismo público. Este representante estará establecido en un Estado miembro deberá atender, en colaboración con el representante (o encargado) a quien representa, las consultas de las autoridades de control y de los interesados sobre el tratamiento y el cumplimiento efectivo de las disposiciones del Reglamento Europeo. Además, será el encargado, junto con el responsable, de llevar el mencionado registro con las actividades del tratamiento, de acuerdo con el artículo 30[139].

137 Artículo 14, definición 17, del Reglamento General de Protección de Datos: "«representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento".

138 Artículo 27 del Reglamento General de Protección de Datos. "Representantes de responsables o encargados del tratamiento no establecidos en la Unión. 1. Cuando sea de aplicación el artículo 3, apartado 2, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión. 2. La obligación establecida en el apartado 1 del presente artículo no será aplicable: a) al tratamiento que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o b) a las autoridades u organismos públicos. 3. El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado. 4. El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento. 5. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado".

139 Ver apartado sobre el responsable del tratamiento y su regulación por parte del Reglamento General de Protección de Datos, en este mismo capítulo.

3.4.- Medidas de seguridad según la normativa de protección de datos

El proveedor *cloud*, atendiendo a la tipología de implementación (pública, privada o híbrida) y a la categoría del servicio contratado (infraestructura como servicio, plataforma como servicio o software como servicio), será responsable de la adopción de medidas de seguridad acordes con la legislación vigente que le sea aplicable, en nuestro caso, en lo referente al Título VIII del Reglamento de desarrollo de la LOPD, que resulta de aplicación en estos momentos. Asimismo, deberá asistir y colaborar con el responsable para que este pueda dar cumplimiento a las obligaciones legales, y permitir el ejercicio de los derechos reconocidos a los titulares de los datos. Dedicaremos este apartado a las obligaciones sobre seguridad en materia de protección de datos de carácter personal, establecidas por nuestro ordenamiento vigente y realizaremos una breve aproximación a su regulación por el nuevo Reglamento europeo.

3.4.1.- Las medidas de seguridad exigidas por la LOPD

Cuando los datos tratados por el cliente y por el proveedor tienen carácter personal, la LOPD y más concretamente, su reglamento de desarrollo, detallan específicas medidas de seguridad que deberán adaptarse, en su caso, a las características propias de los sistemas *cloud*[140].

Con carácter general, la LOPD[141] (art. 9) impone al responsable la obligación de adoptar las medidas de seguridad técnicas y organizativas que permitan garantizar la seguridad de los datos contra pérdidas, alteraciones o accesos no autorizados. En caso de que el responsable externalice parte del tratamiento, en el contrato con el encargado se establecerán las medidas de seguridad que este último esté obligado a

140 En posteriores capítulos analizaremos la seguridad de los sistemas y de los datos migrados desde la perspectiva de las obligaciones contractuales específicas del prestador de servicios *cloud*, y, más concretamente, al mantenimiento de la confidencialidad, integridad y disponibilidad de los datos migrados.

141 Art. 9 LOPD. "El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas".

implementar (art. 12.2 LOPD[142]). Estas medidas aparecen desarrolladas en el Título VIII del RLOPD (art. 70 a 114). La Agencia Española de Protección de Datos[143], por su parte, ha realizado diferentes aportaciones para facilitar su implementación práctica.

Como hemos dicho anteriormente, entre las cargas del empresario que suscribe servicios de computación en la nube para tratar datos personales, como responsable del tratamiento, se encuentra la de elegir un proveedor que ofrezca unas medidas de seguridad técnicas y organizativas adecuadas para permitirle un óptimo ejercicio de sus actuaciones de instrucción y control como responsable[144]. Esta responsabilidad, cuando se produzcan subcontrataciones, debería extenderse a los diferentes subencargados. Por tanto, deberían articularse mecanismos de supervisión que permitan al responsable los controles y comprobaciones pertinentes, teniendo en cuenta que su implementación en determinados servicios no siempre será sencilla, especialmente, cuando sea el encargado del tratamiento quien tenga una posición contractual dominante respecto del cliente responsable del tratamiento[145].

Esta tarea implicará un análisis de riesgos sobre las medidas que, de forma acumulativa, necesitan aplicarse atendiendo al nivel de sensibilidad de los datos (bajo, medio o alto) sometidos a tratamiento. Debemos tener en cuenta, en el caso de servicios contratados por pequeños empresarios, que un mismo servicio de computación en la nube no distinguirá los ficheros según su nivel de sensibilidad de los datos, ni dará opción al cliente responsable del tratamiento para clasificar cada

142 Art. 12.2 LOPD. "(...) En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".

143 Sitio web oficial de la AEPD, en relación a las medidas de seguridad. <https://www.agpd.es/portalwebAGPD/canalresponsable/obligaciones/medidas_seguridad/index-ides-idphp.php> [Fecha de consulta: 22 de septiembre de 2015]. La web de la AEPD también ofrece una Guía sobre la seguridad de los datos [en línea]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf>. [Fecha de consulta: 14 de septiembre de 2016].

144 Así lo impone el art. 20.2 RLOPD: "Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento". A su vez, el Dictamen 5/2010 del GT29, pág. 8, confirma su aplicación en estos términos: "El responsable debe elegir un proveedor que garantice el cumplimiento con la legislación en materia de protección de datos". (Traducción propia).

145 Así lo afirma MIRALLES, quien considera que será complicado implementar estas soluciones especialmente cuando el encargado del tratamiento tenga una posición predominante en el mercado. MIRALLES, Ramón, "*Cloud Computing* y protección de datos" [en línea], *Revista de Internet Derecho y Política de la Universitat Oberta de Catalunya*, núm. 11, 2010. Disponible en: <http://idp.uoc.edu/index.php/idp/issue/view/n11>. [Fecha de consulta: 14 de septiembre de 2016].

fichero en atención al nivel de seguridad requerido, puesto que el proveedor oferta generalmente un servicio homogéneo con medidas de seguridad adecuadas a estándares.

Una solución podría ser la implementación por defecto de medidas de seguridad adecuadas para datos de nivel alto. Correlativamente al nivel de sensibilidad de los datos que almacena el fichero, las medidas de seguridad se clasifican en tres niveles, atendiendo a la necesidad de garantizar la confidencialidad e integridad de la información. Estas medidas de seguridad se aplicarán de modo acumulativo, es decir, las medidas de nivel alto incorporan también las exigencias de las medidas de seguridad correspondientes a los niveles inferiores.

1- Las medidas de nivel alto se aplican a ficheros con datos relativos a origen racial, salud y vida sexual; ideología, religión y creencias; afiliación sindical, datos recabados con fines policiales o datos derivados de actos de violencia de género (art. 81.3 RLOPD)[146]. Para estos ficheros se prevén las medidas de los arts. 101 a 103 del RLOPD, que incluyen la conservación de copias de seguridad en lugar diferente al de las instalaciones internas de los equipos informáticos de la entidad (por ejemplo, una copia de respaldo en la nube), la identificación codificada de soportes, el cifrado y el registro de los accesos a los datos.

2.- Las medidas de nivel medio (art. 81.2 RLOPD) se aplican a datos sobre comisión de infracciones administrativas o penales; prestación de servicios de solvencia patrimonial o crédito (art. 29 LOPD); datos tributarios, financieros y de Seguridad Social; y aquellos datos que describan la personalidad del ciudadano o permitan evaluar su personalidad o comportamiento; así como los datos de telecomunicaciones relativos al tráfico y localización (informe AEPD 160/2004). Estas medidas se recogen en los arts. 95 a 100 del RLOPD, y incluyen, entre otras: la designación de uno o varios responsables de seguridad; la auditoría bianual obligatoria (interna o externa); registros de entrada y salida de soportes y documentos, el acceso físico únicamente a personal autorizado o el registro de incidencias[147].

146 Será suficiente mantener medidas de seguridad básicas para este tipo de datos cuando "a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros. b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad" (art. 81.5 RLOPD).

147 Ver, en este mismo apartado, el subapartado "El responsable de seguridad y el documento de seguridad".

3.- El nivel básico de medidas (art. 81.1 y 89 RLOPD) se aplicará a cualquier otro fichero que contenga datos de carácter personal, y son exigibles en todos los casos. Entre ellas, la realización de copias de respaldo semanales, controles de acceso con diferentes niveles de autorización para los usuarios, o autorización del responsable para permitir la salida de documentos.

A la vista de las medidas de seguridad expuestas, en cuanto a la elección del proveedor, existe el deber, para pequeñas empresas que suscriban servicios *cloud,* y asuman el papel de responsables, de asegurarse de que las medidas implementadas por el proveedor son adecuadas[148]. También deben recabar información sobre cómo pueden ser auditadas estas medidas. Si se emiten certificados de cumplimiento de medidas de seguridad por terceros independientes, el responsable debe conocer la entidad auditora y el tipo de estándares que se aplicarán en la auditoría. Cabe poner de manifiesto la dificultad práctica que encuentran en ocasiones las pequeñas empresas para acceder a esta información, al ser la parte contractualmente más débil.

El cliente debe ser informado diligentemente por el proveedor sobre las incidencias de seguridad que afecten a lo datos personales de los cuales aquel es responsable, así como de las medidas que se adoptarán para resolverlas o de las precauciones que debe tener el cliente para proteger su información o para evitar daños[149]. La puesta en conocimiento del usuario de brechas de seguridad de los sistemas *cloud* que puedan haber afectado a datos personales forma parte del deber de diligencia del proveedor de computación en la nube y, a partir de la aplicación del nuevo Reglamento General de Protección de Datos, una obligación del cliente empresario, en su papel de responsable[150].

Las consecuencias de la no adopción de las medidas de seguridad adecuadas pueden derivar en sanciones para los responsables y encargados del tratamiento[151]

148 Para asegurarse el cumplimiento con la normativa sobre privacidad, la empresa que desee implementar servicios de computación remota puede acudir a guías y recomendaciones realizadas por diferentes entidades, como las citadas publicaciones de ENISA (ENISA, *Cloud Security Guide for...*, *op. cit*. [en línea]) o la AEPD (AEPD, *Guía para clientes que contraten...*, *op. cit*. [en línea]), así como a consultoras independientes.

149 Grupo de Trabajo del Artículo 29, *Dictamen 5/2012 sobre Cloud Computing* (WP 196) y *Opinión 03/2014 sobre la notificación de violación de datos personales*, (WP 213), *op. cit.,* pág. 17.

150 Ver apartado "La seguridad de los sistemas y el plan de emergencia ante incidentes de seguridad como obligaciones de resultado", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

151 Art. 43.1 LOPD. "Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley".

(arts. 44 y 45 LOPD) con importes de elevada cuantía (de 900 a 600.000 €), además de indemnizaciones a los particulares afectados (art. 19 LOPD).

Por último, cabe decir que algunas instituciones, conscientes de la aparente complejidad de la normativa, han elaborado pautas para implementar de forma práctica medidas de seguridad en cuanto a protección de los datos personales[152]. Asimismo, el Grupo de Trabajo del Art. 29 considera en su Dictamen 5/2012 sobre *Cloud Computing* que, además de la integridad y confidencialidad de los datos, las medidas de seguridad para datos almacenados en la computación en la nube deben atender también a otros aspectos relacionados con la seguridad de los datos: la disponibilidad, la transparencia, el aislamiento, la capacidad para ser intervenidos, la portabilidad y la auditabilidad[153].

3.4.2.- El responsable de seguridad y el documento de seguridad

En nuestra normativa sobre protección de datos aparece, como figura diferenciada del responsable del tratamiento, el responsable de seguridad[154]. En el art. 5.2.l) del RLOPD se le define como " persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables", y es precisamente esta norma la que contempla tal figura, cuya designación aparece como parte del contenido del denominado "documento de seguridad" (art. 95 RLOPD[155]),

152 En la "Guía para seguridad en la nube para PYME" [en línea], redactada por la Agencia ENISA, se facilitan herramientas para que la pequeña empresa pueda recabar información sobre medidas de seguridad del proveedor. Disponible en: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes>. [Fecha de consulta: 29 de agosto de 2016]. Además, deben tenerse en cuenta las recomendaciones específicas que puedan publicar las diferentes Autoridades nacionales en materia de Protección de Datos, como nuestra AEPD.

153 Para estos aspectos, nos remitimos al ya mencionado Dictamen 5/2012 sobre *Cloud Computing* del Grupo de Trabajo del Artículo 29, y a las consideraciones respecto de algunas de estas cuestiones (concretamente la integridad, la confidencialidad, la disponibilidad y la portabilidad) en capítulos posteriores, respecto de datos de cualquier naturaleza almacenados en la nube, en conexión con la obligación contractual del prestador de servicios *cloud* de conservarlos de manera segura.

154 Recordemos, como hemos dicho al inicio del presente apartado, que deberemos atender si al proveedor *cloud* queda obligado por el RLOPD y, consecuentemente, de su régimen de medidas de seguridad, de acuerdo con su ámbito de aplicación territorial (art. 3 RLOPD).

155 Art. 95 RLOPD. "En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal, o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad. En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento".

el cual debe redactarse, como hemos visto en apartados anteriores, juntamente con la instauración del resto de medidas correspondientes a datos con nivel medio de seguridad.

Esta figura[156] es la encargada del control y supervisión de la implementación de las medidas de seguridad, analizará los informes de las auditorías (cuyo resultado comunicara al responsable del tratamiento, art. 96.3 RLOPD[157]) y, en el caso de datos especialmente sensibles, procederá a la instauración de mecanismos que permitan controlar accesos a tratamientos automatizados, así como de su revisión e informe al responsable del tratamiento (art. 103 RLOPD[158]). En cuanto al nombramiento del responsable de seguridad, que tendrá lugar cuando deban aplicarse medidas de seguridad para datos de nivel medio o alto, la norma determina que corresponderá al responsable proceder a su designación (art. 5.2.l del RLOPD). En la práctica de la prestación de servicios de computación en la nube, sin embargo, sucede que el responsable de seguridad de los datos almacenados en servidores remotos es elegido generalmente por el proveedor *cloud,* por razones de índole práctica, puesto que es en su infraestructura (o, en su caso, en la de un subproveedor) donde tiene lugar el tratamiento de datos[159].

Cuando únicamente se haya externalizado parte del tratamiento de los datos, y el cliente empresario responsable del tratamiento realice también actividades a las cuales corresponda la aplicación de medidas de seguridad, deberá nombrar a su propio responsable de seguridad en relación a aquellos ficheros que gestione dentro de su propia organización. Una vez nombrado, debe aparecer identificado como tal

156 La regulación reglamentaria de la figura del responsable de seguridad ha sido objeto de interpretación por la AEPD. Nos remitimos a su publicación sobre el responsable de seguridad [en línea]. Disponible en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/medidas_seguridad/common/pdfs/1999-0000_Responsable-de-seguridad.pdf>. [Fecha de consulta: 12 de mayo de 2017].

157 Art. 96.3 RLOPD. "Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas".

158 Art. 103 RLOPD. "(...). 3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos. (...). 5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados".

159 SAIZ PEÑA, Carlos A, "Medidas de seguridad en el Cloud Computing", *Derecho y Cloud Computing* (coord. Ricard Martínez), 2012, Navarra, pág. 171.

en el documento de seguridad (art. 88.4.a RLOPD[160]). Lo ideal será que el responsable de seguridad nombrado por la empresa *cloud* se corresponda con una persona que conozca los mecanismos internos de funcionamiento técnico y de seguridad de la compañía y la normativa sobre protección de datos, que tenga recursos suficientes para ejercer ese cargo con solvencia[161]. En el caso de los servicios de computación en la nube, la Agencia Española de Protección de Datos interpreta que el responsable podrá delegar en el proveedor *cloud* encargado la llevanza del documento de seguridad, al cual nos referiremos posteriormente, ya que este es quien se encarga de coordinar y controlar las medidas de seguridad, aunque este extremo deberá aparecer recogido por el contrato suscrito entre proveedor y encargado[162].

El RLOPD afirma que el nombramiento del responsable de seguridad en ningún momento exonera de responsabilidad ni al responsable del tratamiento ni al encargado, figuras comentadas en apartados anteriores. El RLOPD tampoco especifica taxativamente los requisitos que debe cumplir, ni exige que se trate de una figura que no pueda coincidir con alguna de las dos anteriores, sino que únicamente detalla sus funciones. Tampoco aparece esta figura como susceptible de ser sancionada por el régimen de infracciones previsto por la LOPD, como sí sucede con el responsable del tratamiento y el encargado.

La implementación de las aludidas medidas de seguridad se documentará mediante la llevanza actualizada del llamado documento de seguridad (art. 88 RLOPD[163]). Se trata de un documento interno de la entidad, que debe mantenerse actualizado y que debe incluir cierta información, entre la que destaca: la

160 Art. 88.4.a) RLOPD: "4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además: a) La identificación del responsable o responsables de seguridad".

161 SAIZ PEÑA, Carlos A, "Medidas de seguridad en el Cloud ...", *op. cit.,* pág. 171.

162 Dice la AEPD en su *Guía de seguridad de datos* [en línea], pág. 11: "En caso de haber contratado la prestación de servicios por terceros para determinados ficheros, en el documento de seguridad se debe hacer constar esta circunstancia, indicando una referencia al contrato y su vigencia, así como los ficheros objeto de este tratamiento. Si se ha contratado la prestación de servicios en relación con la totalidad de los ficheros y tratamientos de datos del responsable, y dichos servicios se prestan en las instalaciones del encargado del tratamiento se podrá delegar en este la llevanza del documento de seguridad". Disponible en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf>. [Fecha de consulta: 12 de mayo de 2017].

163 Art. 88.1 RLOPD. Documento de seguridad. "El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información".

especificación detallada de las medidas, normas, procedimientos, reglas y estándares de seguridad, las funciones y obligaciones del personal, la estructura y descripción de los ficheros o el procedimiento de notificación, gestión y recuperación de datos en caso de incidentes de seguridad[164] (art. 88.3 y ss RLOPD[165]).

El nuevo Reglamento General de Protección de Datos establece también la llevanza de un registro con todas las actividades de tratamiento efectuadas bajo la responsabilidad del responsable y del encargado (o sus respectivos representantes), que deberá contener, junto a otra información, "cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1". Además, afirma el apartado 4 del mismo artículo que "no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10". Si bien de momento es obligatoria la llevanza actualizada del documento de seguridad en los términos exigidos por la legislación aplicable en la actualidad (art. 88 RLOPD), una vez que el nuevo Reglamento sea de aplicación deberemos estar a la adecuación de la normativa nacional para ver si se mantiene una obligación similar o equivalente a la llevanza del documento de seguridad recogido en la normativa actual o si, por el contrario, esta obligación se relaja en su detalle respecto de las medidas de seguridad adoptadas, como parece desprenderse de la lectura del

164 La AEPD ha publicado en su web diferentes guías y modelos del documento de seguridad, para su implementación práctica por los responsables del tratamiento [en línea]. Disponibles en: <https://www.agpd.es/portalwebAGPD/canalresponsable/guia_documento/index-ides-idphp.php>. [Fecha de consulta: 12 de mayo de 2017].

165 Art. 88.3 y ss RLOPD. "3. El documento deberá contener, como mínimo, los siguientes aspectos: a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos. b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento. c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros. d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan. e) Procedimiento de notificación, gestión y respuesta ante las incidencias. f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados. g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos. 4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además: a) La identificación del responsable o responsables de seguridad. b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento. 5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo. 6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. (...)."

Reglamento europeo.

3.4.3.- Las medidas de seguridad en el nuevo Reglamento europeo

El Reglamento General de Protección de Datos establece varios principios que deberán regir el tratamiento de datos personales en sus artículos 5 a 7. Entre otras exigencias, se requiere que el tratamiento de datos personales garantice su seguridad, especialmente en aquello referente a su integridad y confidencialidad, mediante la aplicación de medidas técnicas y organizativas adecuadas (art. 5.1 del nuevo Reglamento[166]).

Quien deberá cumplir, acreditar y responder por el cumplimiento de estos principios y, por ende, de la adopción de medidas técnicas y organizativas adecuadas, será el responsable del tratamiento[167]. Cualquier persona que actúe bajo su responsabilidad (empleados del responsable, encargados del tratamiento y sus empleados, etc.) y tenga acceso a datos personales únicamente actuarán, salvo norma en contrario, bajo las instrucciones del responsable. El responsable y el encargado deberán asegurarse de que así sea (art. 32.4 del Reglamento europeo[168]).

En referencia a la obligación del responsable del tratamiento y, en su caso, del encargado, de aplicar medidas técnicas y organizativas que garanticen un nivel de seguridad adecuado, el Reglamento europeo establece varios aspectos a tener en consideración en su artículo 32[169].

---

166 Artículo 5.1.f) del Reglamento General de Protección de Datos. "1. Los datos personales serán: (...) f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

167 Artículo 5.2 del Reglamento General de Protección de Datos. "2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".

168 Artículo 32.4. del Reglamento General de Protección de Datos. "El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

169 Artículo 32 del Reglamento General de Protección de Datos. "1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: a) la seudonimización y el cifrado de datos personales; b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; d) un

En primer lugar, se refiere al estado de la técnica en cuanto a mecanismos destinados a proteger la integridad y la confidencialidad de los datos personales. En el campo de la computación en la nube, el proveedor, como encargado del tratamiento de los datos personales migrados por el cliente-pequeño empresario, deberá barajar las posibilidades y mecanismos técnicos aplicables a los sistemas de almacenamiento y red, por ejemplo, mecanismos físicos y de software informático que permitan una protección de la integridad de los datos digitales e imposibiliten el acceso a esos datos a terceros no autorizados. En cuanto al responsable del tratamiento-pequeño empresario, deberá igualmente adoptar los mecanismos técnicos que estén a su alcance para minimizar tales riesgos, como puedan ser controles de acceso a los sistemas informáticos de la organización, la realización de copias de respaldo que impidan la pérdida de datos y faciliten su recuperación o la instalación de *suites* de seguridad (antivirus, cortafuegos, y otros mecanismos preventivos ante amenazas de carácter informático), y una adecuada gestión de la seguridad física respecto de los soportes y documentos que contengan datos personales. También deberá atenderse a las funciones y obligaciones del personal que realiza el tratamiento, debiendo estar definidas y documentadas en el registro de actividades de tratamiento, obligación recogida en el artículo 30.

Asimismo, se tendrán en cuenta los costes asociados a esa implementación y la posibilidad realista del obligado en cuanto a su adopción, mantenimiento e implementación práctica.

Otros aspectos a considerar en cuanto a la adopción de medidas de seguridad según el Reglamento europeo son la naturaleza, el alcance, el contexto y los fines del tratamiento, que irán ligados a la actividad de la organización que los trate y a los riesgos para los derechos de los interesados que se deriven de ese tratamiento[170].

---

proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. 2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. 3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo. 4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

170 En el caso de pequeñas empresas turísticas, los datos tratados estarán relacionados con las preferencias y gustos en cuanto a alojamiento y restauración, datos personales y de facturación de

El mismo artículo 32 del Reglamento europeo recomienda algunas de las medidas que pueden adoptarse en atención a la probabilidad y gravedad de los riesgos para la privacidad de los interesados que provocaría su destrucción, pérdida o alteración accidental o ilícita. Se trata de medidas especialmente pensadas para datos contenidos en soportes digitales.

Así, en primer lugar, destaca la seudonimización, que aparece definida en su artículo 4.5 como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable". Esta técnica ya fue examinada por el Grupo de Trabajo del Artículo 29 en su Dictamen 5/2014 sobre técnicas de anonimización, concluyendo que estas técnicas tienen sus ventajas e inconvenientes (especialmente, limitaciones técnicas), pero que, si tienen un diseño adecuado, resultan un buen sistema para garantizar la privacidad de los datos[171].

Igualmente, recomienda que los sistemas informáticos, aplicaciones y servicios destinados al tratamiento de datos de carácter personal incorporen las suficientes garantías desde el momento en que son diseñados e implementados, en cuanto a garantizar su confidencialidad, integridad, disponibilidad y resiliencia (art. 32.1.b) ; y a permitir la recuperación y el acceso a los datos de manera rápida en caso en que se produzca un incidente físico o técnico (art. 32.1.c). Igualmente, todas las medidas implementadas deberían poder ser auditables y deberían someterse a una evaluación de su eficacia de manera periódica para controlar su efectividad como

---

los clientes, así como información que puede tener carácter personal relacionada con proveedores y empleados. Sin embargo, con el fin de proporcionarles a sus clientes un servicio individualizado y de mayor calidad, existirán establecimientos que recaben datos de salud (por ejemplo, una intolerancia alimentaria o algún tipo de alergia conocida, discapacidades motoras, etc.), que requieran unas medidas de seguridad más estrictas. La información puede encontrarse en soporte documental, o digital, alcanzando archivos de texto o datos introducidos en programas informáticos hasta imágenes de videovigilancia, y restringirse al ámbito del propio establecimiento o transmitirse a socios comerciales, terceras empresas o autoridades competentes. Todos estos aspectos serán importantes a la hora de determinar qué medidas son suficientes y adecuadas para garantizar al máximo la confidencialidad de los clientes. Ver capítulo "La contratación de servicios de *Cloud Computing* por el pequeño empresario turístico".

171 Para más información sobre las técnicas de anonimización y seudonimización, nos remitimos al apartado "Algunas medidas relacionadas con el borrado: la cláusula de confidencialidad, la anonimización y la seudonimización", en el capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube", y al Dictamen 5/2014 sobre técnicas de anonimización elaborado por el Grupo de Trabajo del Artículo 29 [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf>. [Fecha de consulta: 12 de mayo de 2017].

garantía de seguridad (art. 32.1.d).

Los códigos de conducta, sellos de calidad y otros mecanismos de certificación suficientemente acreditados a tenor del artículo 40 podrán demostrar la adecuación de las medidas de seguridad al efectivo tratamiento realizado y el cumplimiento de la obligación del responsable y, en su caso, del encargado, respecto de la adopción de medidas técnicas y organizativas adecuadas (art. 33.3 del Reglamento europeo)[172]. Respecto de la computación en la nube, podemos destacar el Código de Conducta en materia de Protección de Datos del C-SIG (*Cloud Select Industry Group*)[173]. Con todo, debemos recordar que este código de conducta se adoptó bajo la vigencia de la Directiva 95/46, con lo cual opinamos que deberá adaptarse al nuevo Reglamento en todo aquello que sea necesario para que pueda mantener todas las garantías una vez que este sea de aplicación.

3.5. El papel de las autoridades y de terceros independientes en materia de protección de datos

Hasta ahora, hemos hablado de las diferentes categorías jurídicas que la LOPD atribuye a los diferentes operadores relacionados contractualmente en cuanto al tratamiento de datos de carácter personal. A continuación, estudiaremos el papel que tienen otras persones o entidades que también son relevantes en cuanto a la normativa vigente en materia de protección de datos.

172 Respecto de los diferentes mecanismos de autorregulación y la normativa referente a códigos de conducta, sellos y marcas, nos remitimos al excelente trabajo realizado por VIGUIRI CORDERO, Jorge; "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo Derecho europeo en protección de datos,* Valencia, 2015, págs. 901 a 957. Sobre las mismas cuestiones, con especial referencia a la autorregulación en las redes sociales y la protección de datos personales, TRONCOSO REIGADA, Antonio; *La protección de datos personales. En busca del equilibrio*, 1ª edición, Valencia, 2010, págs. 1708 y ss.

173 Este código de conducta, que está siendo elaborado por representantes del sector de la industria del *Cloud Computing* (*Cloud Select Industry Group* o C-SIG), sometido a revisión por el Grupo de Trabajo del Artículo 29 y promovido por la Comisión Europea, pretende dar uniformidad en la aplicación de la normativa en materia de protección de datos por parte de los proveedores de servicios de computación en la nube. En la fecha de conclusión de este trabajo, la redacción de este código de conducta se halla en su etapa final, aunque no se ha publicado el documento definitivo. Información disponible en: <https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct> y <https://ec.europa.eu/digital-single-market/en/news/opinion-article-29-data-protection-working-party-code-conduct-data-protection-cloud-service>. [Fecha de consulta: 9 de mayo de 2017].

Como hemos mencionado en apartados anteriores, la Directiva 95/46/CE, en su Considerando 62, establece que la figura de la autoridad de control es un garante esencial en la materialización de la protección de datos[174]. La Agencia Española de Protección de Datos se encarga de velar por el cumplimiento de la normativa, y en especial, por el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, comúnmente conocidos como derechos ARCO, como se verá más adelante. Es un Ente de Derecho público, con personalidad jurídica propia y dependiente del Ministerio de Justicia.

Entre sus principales funciones, se encuentran la atención a los afectados (información y resolución de reclamaciones), la emisión de autorizaciones de tratamiento y transferencia de datos u órdenes para su cese y cancelación, el ejercicio de la potestad sancionadora que le otorga el Título VII de la LOPD, la elaboración de informes en cuestiones normativas relacionadas con la protección de datos, la tutela de los derechos de los usuarios en el ámbito de las comunicaciones electrónicas y la cooperación con otros organismos comunitarios e internacionales en materia de protección de datos[175].

En el Reglamento General de Protección de Datos se mantienen el concepto de autoridad de control como "la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51" (artículo 4. 21), y estableciéndose la obligación para los Estados miembros de la designación de una o varias autoridades de control. Su actuación se llevará a cabo con total independencia y desempeñará sus funciones sin injerencias u órdenes de otros organismos públicos o privados (art. 52 del Reglamento[176]).

---

174 Ver apartado "Marco normativo de la protección de datos", en este mismo capítulo.

175 Para conocer las funciones de la AEPD, puede visitarse la información publicada en su página web oficial, así como un listado de todos los países del mundo que cuentan con autoridad en materia de protección de datos. Disponible en: <http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/funciones-ides-idphp.php> y en: <http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/common/Paises_autoridad_Proteccion_Datos_Miembro_Conferencia_Internacional.pdf>. [Fecha de consulta: 12 de mayo de 2017].

176 Artículo 52 del Reglamento General de Protección de Datos. "1. Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento. 2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción. 3. El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad

Volviendo a la normativa vigente, el art. 96 del Reglamento de desarrollo de la LOPD obliga a la realización de una auditoría bianual interna o externa, por parte de un experto en la LOPD, que verifique el cumplimiento de las obligaciones en cuanto a medidas de seguridad cuando se almacenen datos con una sensibilidad de nivel medio o alto. También será obligatoria una auditoría extraordinaria cuando se realicen modificaciones sustanciales en los sistemas de información que puedan afectar al cumplimiento de medidas de seguridad[177]. Existen empresas y otras entidades[178] que se encargan de la realización de estas auditorías externas y que expiden certificados independientes, y una vez obtenido su informe, deberá conservarse hasta la realización del posterior[179].

Estas verificaciones y certificados independientes realizados por profesionales expertos facilitarán al proveedor de servicios *cloud* y al cliente empresario responsable del tratamiento la prueba del cumplimiento legal de sus obligaciones en materia de de protección de datos ante las autoridades de control, interesados y terceros que así se lo requieran. Sin embargo, la norma vigente no impide que el proveedor *cloud* se audite a sí mismo en materia de protección de datos, como

---

profesional que sea incompatible, remunerada o no. 4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité. 5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada. 6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional".

177 Art. 96 RLOPD. "A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título. Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior. 2.- El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas".

178 A modo de ejemplo, citar las empresas españolas Iniciem Consultores o Datusmas, así como otros muchos profesionales independientes que realizan tareas de consultoría y verificación.

179 Respuesta a la consulta realizada a la AEPD sobre cuánto tiempo debe conservarse el informe sobre la auditoría en materia de medidas de seguridad. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/medidas_seguridad/common/pdfs/2010-0191_Plazo-de-conservaci-oo-n-de-informes-de-auditor-ii-a-de-seguridad.pdf>.[Fecha de consulta: 9 de mayo de 2017].

tampoco que la realice el responsable del tratamiento[180]

Los clientes de servicios *cloud* que actúan como responsables, deberían poder exigir, en opinión del Grupo de Trabajo del Artículo 29 y conforme al criterio que compartimos, una copia de estos informes, como cumplimiento de la obligación de control del responsable[181]. Tengamos en cuenta que resulta impracticable una verificación de la infraestructura de servidores físicos y virtuales por parte de todos los responsables de datos que comparten el hardware del proveedor o de sus subproveedores, no solo porque a menudo estos servicios se comercializan masivamente, sino también porque puede poner en riesgo la seguridad lógica y física del sistema y de la red que suministran el servicio. El Grupo de Trabajo del Art. 29 también estima que estas certificaciones deberían indicar, como mínimo, que los controles se han realizado teniendo en consideración los estándares reconocidos[182]

Para una efectiva relación de confianza entre proveedores *cloud*, responsables y titulares de datos personales, el Grupo de Trabajo del Artículo 29 considera clave la adopción de estándares y certificados específicos en materia de privacidad, que incluyan medidas técnicas (como la localización de los datos o su encriptado) así como procesos que garanticen la protección de tales datos (como políticas de control de accesos o copias de seguridad).

Al respecto, el nuevo Reglamento establece una regulación más estricta de las entidades responsables de códigos de conducta. A la vez que promueve su creación y adopción, especialmente en cuanto a la atención de las necesidades de los diferentes sectores empresariales y a su envergadura (art. 40.1[183]), el Reglamento europeo impone la obligación de remitir a la autoridad de control competente las propuestas, modificaciones o ampliaciones de códigos de conducta en materia de protección de datos para aquellas asociaciones y entidades representativas de los distintos sectores

180 SAINZ PEÑA, Carlos A, "Medidas de seguridad...", *op. cit.*, pág. 173.

181 Dictamen 5/2012 del Grupo de Trabajo del Artículo 29 sobre el *Cloud Computing* (WP 196), pág. 22.

182 Los estándares mencionados por el Dictamen 5/2012 del Grupo de Trabajo del Artículo 29 (pág. 22) son los estándares ISO 27018 (*International Standards Organisation*), la *International Auditing and AssuranceStandards Board* y la *Auditing Standards Board of the American Institute of Certified Public Accountants.*

183 Artículo 40.1 del Reglamento General de Protección de Datos. "1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas".

empresariales que integren a responsables y encargados del tratamiento, con el fin de que la autoridad de control dictamine su adecuación al Reglamento europeo y la suficiencia de sus garantías (art. 40.5[184]). Una vez aprobado este código de conducta, la autoridad competente procederá a su registro y publicación. Además, el cumplimiento con este código de conducta se comprobará mediante una supervisión periódica por un organismo independiente que a tal efecto habrá sido acreditado por la autoridad de control, y tomar medidas cuando se produzcan infracciones por un responsable o encargado, entre ellas la suspensión o expulsión del infractor (art. 41.4[185]).

En nuestra opinión, era necesario establecer un cierto control de calidad sobre los mecanismos de certificación y códigos de conducta existentes en materia de protección de datos, dada su proliferación y su falta de homogeneidad y supervisión, con lo cual aplaudimos la regulación efectuada por el Reglamento. Sin embargo, consideramos deseable, especialmente en respuesta a la necesidad de dinamismo que exigen los servicios de computación en la nube y el cumplimiento de la normativa de protección de datos personales, que la obtención de estas certificaciones y la adhesión a los códigos de conducta por parte de los clientes pequeños empresarios responsables del tratamiento se pueda realizar a través de un procedimiento ágil y que sean económicamente asequibles.

3.6.- Los derechos del interesado

El empresario que contrate servicios de computación en la nube, como responsable del tratamiento, está obligado a permitir el ejercicio de los derechos de acceso, rectificación, cancelación y oposición que ostentan los titulares de los datos,

184 Artículo 40.5 del Reglamento General de Protección de Datos. "Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas".

185 Artículo 41.4 del Reglamento General de Protección de Datos. "Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente".

de acuerdo con los artículos 15 a 17 de la LOPD. Igualmente, cuando sea de aplicación el Reglamento General de Protección de Datos, deberá atender a otros derechos del interesado que se reconocen de manera novedosa: el derecho de supresión y su conexo derecho al olvido, el derecho a la limitación del tratamiento, el derecho a la portabilidad de los datos y el derecho a ser informado sobre brechas de seguridad. Para llevar a cabo esta tarea, será necesaria la colaboración entre el cliente-responsable y el prestador *cloud* encargado del tratamiento. El pequeño empresario que sea cliente *cloud*, por tanto, deberá asegurarse de que el proveedor está dispuesto a facilitarle la información y herramientas adecuadas que le permitan cumplir los plazos legales y atender al ejercicio diligente de estos derechos[186].

A continuación, dedicaremos unas líneas a cada uno de estos derechos y a su ejercicio en el ámbito de la computación en la nube.

3.6.1.- Los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO)

Los derechos de acceso, rectificación, cancelación y oposición, denominados ARCO por el acrónimo que forman sus iniciales, solo pueden ejercerse por el interesado o su representante legal y deben poder hacerse efectivos de forma gratuita (art. 17.2 LOPD). Las solicitudes motivadas para su ejercicio deberán dirigirse al responsable del fichero, quien deberá resolver sobre lo solicitado en los plazos legales. En caso de que la solicitud no haya sido atendida en plazo, o que haya sido denegada, el solicitante podrá dirigirse a la AEPD, para que requiera medidas de corrección. Trasladando esta situación a la relación existente entre la empresa cliente de servicios *cloud* y su proveedor, implicará que el cliente deberá hacerse cargo de las solicitudes que le presenten los interesados, y que el proveedor deberá facilitar al máximo el ejercicio de estos derechos.

Veamos el contenido de estos derechos en la normativa aplicable y en el Reglamento General de Protección de Datos recientemente aprobado, así como su traslado al contexto de los servicios de *Cloud Computing*.

1.- El derecho de acceso. Se recoge en el art. 15 de la LOPD[187] y en los arts. 23

186 "El responsable está obligado a hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de 10 días" (art. 16 LOPD).

187 Art. 15 LOPD. Derecho de acceso. "El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.2. La información podrá

a 26 y 27 a 30 del RLOPD, y permite al ciudadano obtener información sobre los datos que le atañen, con la intención de que pueda controlar su uso y la finalidad de su tratamiento. Este derecho no puede ser ejercitado en intervalos inferiores a 12 meses, salvo que se acredite un interés legítimo.

En el Reglamento General de Protección de Datos, este derecho de acceso aparece recogido en su artículo 15, de forma más amplia que en la Directiva 95/46/CE, ya que se reconoce no solo el derecho a conocer la información sobre sus datos, sino la confirmación sobre si resultan o no sometidos a tratamiento, y ciertos extremos sobre ese tratamiento, en especial la finalidad del tratamiento, las categorías de datos afectadas, los destinatarios, el plazo durante el cual los conservará el responsable, la existencia de los derechos de supresión, rectificación, limitación y oposición, la posibilidad de reclamar ante una autoridad de control, información sobre el origen de los datos y de las garantías en caso de que sean transferidos internacionalmente[188].

Su ejercicio en el ámbito de la computación en la nube de acuerdo a la actual Ley Orgánica de Protección de Datos implica que el cliente empresario responsable del tratamiento, ante la petición de información del titular, le facilite o le permita

---

obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes".

188 Artículo 15 del Reglamento General de Protección de Datos. "1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información: a) los fines del tratamiento; b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; f) el derecho a presentar una reclamación ante una autoridad de control; g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. 2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia. 3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. 4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros".

visualizar aquellos datos personales incluidos en el fichero virtual y la finalidad de su tratamiento, el origen de dichos datos y a quién se le han comunicado o se prevén comunicar.

Una vez sea de aplicación el nuevo Reglamento, debe proporcionarse al interesado la información que solicite sobre su tratamiento, lo cual incluirá todos los aspectos detallados por el artículo 15. Además, podrá obtener una copia de los datos personales objeto de tratamiento, no necesariamente gratuita. Puesto que toda esta información debe ser proporcionada al interesado por el cliente empresario responsable del tratamiento, este, como tal, deberá haber recabado previamente del proveedor *cloud* detalles sobre el tratamiento que llevará a cabo a modo de prestación del servicio, no solo con el fin de atender al derecho de acceso de cualquier interesado, sino también, y de manera previa a la contratación, como comprobación de la pertinencia del tratamiento y de la solvencia del proveedor en su papel de encargado.

El ejercicio de estos derechos por parte del titular nunca implicará que pueda acceder a datos de terceros, por ejemplo de otros titulares con quienes se comparta fichero virtual o servidor *cloud,* puesto que los derechos y libertades de otros deben quedar igualmente protegidos (arts. 10 y 11 LOPD, y art. 15.4 del Reglamento europeo).

2.- Los derechos de rectificación y cancelación. El derecho de rectificación permite la corrección de errores y modificar datos que sean inexactos o incompletos. En el Reglamento europeo, mientras el derecho de rectificación mantiene prácticamente su mismo contenido, en el artículo 16, el derecho de cancelación ha cambiado su denominación y su alcance, como veremos a continuación[189].

En la regulación de la Directiva 95/46/CE y en la normativa española se reconoce al interesado el llamado derecho de cancelación, regulado específicamente en los artículos 16.3 de la LOPD y 21 a 33 del RLOPD[190]. Este derecho consiste,

189 Artículo 16 del Reglamento General de Protección de Datos. "El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional".

190 Artículo 16.3 de la Ley Orgánica de Protección de Datos: "La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión". Artículo 31.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley

básicamente, en la supresión de datos inadecuados o excesivos para los fines por los cuales fueron recogidos, previa solicitud del interesado[191].

El derecho de cancelación puede exigirse con independencia del sistema de almacenamiento empleado. Si este almacenamiento es automatizado y tiene lugar en diferentes servidores, dispersos en localizaciones diferentes, como sucede con los sistemas redundantes de la mayoría de entornos de computación en la nube, será necesario asegurar el ejercicio de este derecho en todos los equipos en los cuales pueda almacenarse una copia.

Como se verá en capítulos posteriores, en la práctica generalizada esta supresión no se produce de manera inmediata (porque se necesita un tiempo para que tenga lugar una sobreescritura de datos suficiente para que esa información sea irrecuperable, o para que se borren todos los fragmentos de datos que puedan haberse dispersado debido a motivos técnicos), con lo cual las garantías que puede ofrecer el responsable sobre este borrado y que exigen la Directiva y la Ley Orgánica de Protección de Datos no son totales. Además, debe tenerse en cuenta que el control sobre el procedimiento técnico del borrado lo ostenta el proveedor de servicios de computación en la nube, mientras que la empresa que utiliza los entornos de nube para el tratamiento, como responsable, ciertamente tiene limitaciones técnicas para exigir y, sobre todo, para comprobar la efectividad del cumplimiento del derecho de cancelación en toda su extensión, aunque gran parte de las consecuencias legales recaigan sobre su persona.

El Grupo de Trabajo del Artículo 29 interpretó que el cumplimiento de este derecho de cancelación en ámbitos de computación en la nube implicaba la destrucción o desmagnetización de los soportes físicos de la información, aunque también se permitían procesos de sobreescritura[192]. Como observaremos, tanto la desmagnetización como la destrucción del *hardware* impiden su posterior

---

Orgánica de Protección de Datos: "El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento".

191 Artículo 32.1 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos: "La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado. En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso".

192 Dictamen del Grupo de Trabajo del Artículo 29 núm. 5/2012 sobre *Cloud Computing* (WP 136) [en línea], *op. cit.*, pág. 14.

reutilización[193]. En nuestra opinión, si bien son los mecanismos que ofrecen las mayores garantías a día de hoy, son poco viables técnica y económicamente para la mayoría de proveedores de computación en la nube pública, especialmente para aquellos que prestan servicios de bajo coste y consumo masificado, en otras palabras, aquellos servicios mayoritariamente contratados por particulares, profesionales y pequeños y medianos empresarios.

En cuanto a la opción de la sobreescritura, el Grupo de Trabajo del Artículo 29 exige que se utilicen programas especiales para ello, con la finalidad de que sean suficientes las capas para no permitir la recuperación de los datos. Este proceso de sobreescritura, por otra parte, puede no tener lugar de manera inmediata y automática, especialmente si consideramos la posibilidad de replicados en diferentes centros de datos. Así las cosas, el responsable del tratamiento, obligado a garantizar una supresión segura, deberá aferrarse a la colaboración del proveedor *cloud* y de lo establecido en el clausulado del contrato suscrito entre ambos en sus condiciones de responsable y encargado, para poder exigir del proveedor el máximo alcance del derecho de cancelación ejercitado por el titular, y algún tipo de acreditación o prueba que demuestre que la petición efectuada por el interesado ha sido convenientemente atendida.

Otro aspecto que hay que recordar en cuanto al derecho de cancelación es que el responsable tiene la obligación de informar al interesado sobre la existencia de este derecho, y su posibilidad de ejercitarlo de manera sencilla y gratuita (artículo 13.2.b) de la Directiva 95/46/CE, artículo 5.1.d) de la LOPD y apartados 2 y 3 del artículo 24 del RLOPD). En ese caso, el responsable dispondrá de un plazo de 10 días para atender esta petición, y posteriormente, deberá suprimir los datos (art. 32.3 RLOPD).

Como se ha dicho, en el Reglamento europeo ha desaparecido la terminología del derecho de cancelación, y se ha substituido por el denominado "derecho de supresión", que puede aplicarse de manera genérica, y el llamado "derecho al olvido", que de forma específica se refiere a la supresión de contenidos digitales de carácter personal que se han hecho públicos. Al ser derechos introducidos de manera novedosa por el Reglamento europeo, les dedicaremos expresamente un apartado en este mismo capítulo.

193 Ver apartado "La preservación de datos y su borrado una vez extinguida la relación contractual", en el capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

3.- El derecho de oposición. El derecho de oposición es el derecho del afectado a que no se proceda o se continúe con el tratamiento de sus datos de carácter personal "a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario. b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación y c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento". Aparece regulado en los arts. 6.4, 17 y 30.4 de la LOPD, y en los arts 23 a 26 y 34 a 36 del RLOPD. El responsable dispone de un plazo de 10 días desde la recepción de la solicitud para hacerlo efectivo, excluyendo al titular del tratamiento de datos o denegando motivadamente la petición.

El Reglamento General de Protección de Datos recoge el derecho de oposición en su artículo 21. Supone para el responsable la paralización del tratamiento de los datos personales del interesado, salvo que pueda acreditar que los reserva para efectuar posteriores reclamaciones o pruebe motivos legítimos imperiosos susceptibles de prevalecer sobre los derechos y libertades de aquel. Una novedad de la regulación de este derecho por el Reglamento europeo es su puesta en conexión con aquellos tratamientos dedicados a la mercadotecnia, es decir, que tengan finalidades comerciales y publicitarias, entre ellas la elaboración de perfiles de consumo, ante el cual un interesado podrá oponerse en todo momento.

Respecto de los derechos ARCO, la Agencia Española de Protección de Datos pone a disposición de los titulares, en su página web, diferentes formularios de solicitudes para que puedan dirigirlos a los responsables del tratamiento (y estos, a su vez y en nuestro caso, a los proveedores *cloud* encargados del tratamiento) y materializar el ejercicio de estos derechos. La gestión por parte del cliente *cloud* (responsable del tratamiento) de la petición de acceso, rectificación, cancelación u oposición se realiza, generalmente, por comunicación electrónica, por escrito o telefónicamente, a través del departamento que el proveedor *cloud* pone a disposición del cliente, por ejemplo, el departamento comercial, de atención al usuario o el departamento jurídico. Independientemente de la forma en la cual se posibilite el ejercicio de estos derechos, la Agencia Española de Protección de Datos considera que el cliente deberá verificar que el proveedor no impone obstáculos técnicos y de organización para que pueda tener lugar el ejercicio de los derechos ARCO, así como la efectiva supresión y bloqueo de los datos una vez finalizado su

tratamiento. Igualmente, la AEPD afirma que el contrato entre cliente y proveedor deberá precisar, para ser conforme con los requisitos de la LOPD, la obligación de colaborar con el cliente responsable del tratamiento en cuanto a facilitar el ejercicio de los derechos de los interesados y a garantizar que puedan seguir ejerciéndose ante eventuales subcontratistas.

Además de estos derechos, existen, como hemos comentado al tratar sobre el consentimiento del titular de los datos, el derecho de información previo al tratamiento, contenido en el art. 5 de la LOPD; y el derecho de indemnización, contenido en el art. 19 de la LOPD, al margen de las actuaciones sancionadoras de la AEPD, y que permite reclamaciones ante responsables de ficheros de titularidad pública o privada por la vía jurisdiccional que corresponda, por resarcimiento de daños y perjuicios provocados por un tratamiento inadecuado o ilegítimo de sus datos personales[194].

3.6.2.- Los nuevos derechos reconocidos en el Reglamento General de Protección de Datos. Especial referencia al derecho a la portabilidad y a su aplicación en los servicios de computación en la nube

El Reglamento General de Protección de Datos ha reconocido nuevos derechos para el interesado, que son, además de la ampliación del derecho de información (arts. 12 a 14), el derecho a la limitación del tratamiento (art. 18), el derecho de supresión y el derecho al olvido (art. 17), y el derecho a la portabilidad de los datos (art. 20)[195]. Estos nuevos derechos se suman a los derechos de acceso (art. 15), rectificación (art. 13) y oposición (art. 21), ya recogidos por la LOPD, que tendrán una nueva redacción en el Reglamento europeo, como se ha visto en el apartado precedente.

1.- El derecho a la limitación del tratamiento se regula en el artículo 18 del

194 La Decisión de la Comisión Europea de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, obliga a acordar que los interesados que hayan sufrido daños tendrán derecho a percibir una indemnización a cargo del exportador: "Las partes acuerdan que los interesados que hayan sufrido daños como resultado del incumplimiento de las obligaciones mencionadas en la cláusula 3 o en la cláusula 11 por cualquier parte o subencargado del tratamiento tendrán derecho a percibir una indemnización del exportador de datos para el daño sufrido". Además, añade responsabilidades subsidiarias para cuando no sea posible reclamar al exportador.

195 Nos remitimos, respecto del derecho de información del interesado, a las obligaciones del responsable del tratamiento que le son correlativas, y que han sido analizadas en el apartado "El titular de los datos y la prestación de consentimiento informado e inequívoco", en este mismo capítulo.

Reglamento General de Protección de Datos[196]. El Reglamento define en su artículo 4 la limitación del tratamiento como "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro". Este derecho opera en los casos en los que existe una colisión entre el derecho del interesado a oponerse al tratamiento de sus datos personales y los motivos legítimos del responsable de efectuar ese tratamiento. Supone que, a petición del interesado, no se aplicarán las operaciones de tratamiento a los datos personales del interesado, pero seguirán conservándose por el responsable, quien únicamente podrá utilizarlos para la formulación, ejercicio o defensa de reclamaciones, para proteger los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión Europea o del Estado miembro correspondiente[197]. Respecto de otros aspectos del tratamiento, necesitará del consentimiento expreso del interesado.

En virtud de este derecho, el interesado podrá limitar el tratamiento en cuanto a aspectos que resulten inexactos o no veraces, mientras el responsable determina si accede o no a su solicitud de rectificación. Asimismo, sirve de alternativa al interesado respecto del ejercicio del derecho a la supresión de los datos personales, cuando prefiera optar por que no se proceda a su borrado (por ejemplo, cuando el responsable ya no los necesite para los fines del tratamiento pero el interesado los requiera para realizar reclamaciones). También sirve para que el interesado pueda limitar el tratamiento de los datos mientras el responsable determina si accede o no a una solicitud a la oposición al tratamiento efectuada por el interesado.

196 Artículo 18 del Reglamento General de Protección de Datos: "1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado. 2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación".

197 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía del Reglamento General de Protección de Datos para responsables de tratamiento* [en línea], pág. 11. Disponible en: <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf>. [Fecha de consulta: 15 de mayo de 2017].

Igualmente, el responsable deberá informar a los destinatarios a quienes haya comunicado los datos personales del interesado, de cualquier rectificación, limitación o supresión de datos personales resultante del ejercicio de los derechos homónimos, siempre y cuando no implique esfuerzos desproporcionados. Igualmente, informará al interesado que lo solicite sobre estos destinatarios (art. 19 del Reglamento europeo[198]).

2.- El derecho de supresión (y el derecho al olvido). Como decíamos anteriormente, el derecho de cancelación ha sido substituido en el Reglamento europeo por los llamados "derechos de supresión" y "derecho al olvido". Aunque en la nueva normativa aparecen recogidos como un único derecho para el interesado y se articulan como dos apartados del mismo artículo 17, consideramos el derecho de supresión y el derecho al olvido son dos facultades diferenciables, siendo la segunda una manifestación de la primera, puesto que el derecho al olvido operará específicamente cuando la información personal se hayan hecho públicos a través de la Red (por ejemplo, a través de enlaces en sitios web o de resultados de búsquedas de contenidos), mientras que el derecho de supresión se aplicará en relación al resto de tratamientos que no sean accesibles para el público en general[199].

Así, por una parte, el derecho de supresión de los datos recoge el testigo del tradicional derecho de cancelación, y se reconoce en el apartado primero del artículo 17 del Reglamento[200]. Consiste en la potestad del interesado de exigir que los datos

198 Artículo 19 del Reglamento General de Protección de Datos: "El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita".

199 AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía del Reglamento General de Protección de Datos para responsables de tratamiento* [en línea], pág. 11. Disponible en: <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf>. [Fecha de consulta: 15 de mayo de 2017].

200 Artículo 17.1 del Reglamento 2016/679 General de Protección de Datos: "El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de

personales que le atañen se supriman sin dilación indebida, y puede ejercitarse ante el responsable del tratamiento. El responsable, por su parte, atenderá a la petición del interesado si esta se sujeta a alguna de las condiciones que el mismo artículo enumera: que ya no sea necesario su tratamiento de acuerdo con la finalidad de su recogida, que el interesado proceda a retirar su consentimiento o se oponga al tratamiento de esos datos, que el tratamiento se haya realizado de manera ilícita, que otra norma vigente exija su supresión por parte del encargado, o que se hayan obtenido en relación a una oferta de servicios recibida por un menor de 16 años. El empresario a quien se solicite la supresión de datos que se traten (entendiendo el tratamiento en sentido amplio) en el entorno de nube de un proveedor, debe requerir a este para que bloquee el acceso a esos contenidos desde sus sistemas con la mayor celeridad, y debe exigir su colaboración como encargado del tratamiento, a fin de poder dar cumplimiento al derecho ejercitado por el titular. En caso contrario, pueden devengarse las sanciones administrativas que prevé la misma normativa (Título VII de la LOPD), y, además, compensaciones para los eventuales interesados damnificados (art. 19 LOPD).

Por otra parte, el derecho al olvido, contemplado en el apartado segundo del mismo artículo 17, se relaciona con datos personales que se han hecho públicos[201]. Este artículo reconoce el derecho a eliminar los enlaces o copias de esos datos, bajo las mismas condiciones a las que se sujeta el derecho de supresión del apartado primero, exigiendo al responsable de tratamiento que informe al proveedor, en la medida en que sea técnicamente posible, de la existencia de tales enlaces o copias y de la voluntad del interesado de que se eliminen, para impedir el acceso al público a tales datos.

El derecho al olvido, inicialmente pensado para retirar el acceso a cierta información personal que facilitan metabuscadores en la red o sitios web, puede aplicarse extensivamente a ciertas categorías de servicios de computación en la nube, en especial aquellas que permiten compartir y difundir contenidos en Internet, como las redes sociales[202], así como a otras Webs 2.0 que dispongan de esta

---

la información mencionados en el artículo 8, apartado 1".

201 Artículo 17.2 del Reglamento 2016/679 General de Protección de Datos: "Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos".

202 Respecto de la consideración de las redes sociales como servicios de *Cloud Computing*, nos

funcionalidad[203]. A nuestro parecer, la virtualidad del derecho al olvido en ámbitos de computación en la nube contratados por particulares dependerá de si puede entenderse que un dato personal se ha hecho público a través del uso del servicio *cloud*, ya que, cuando la información personal (o sus enlaces, copias, etc.) se haya distribuido entre un conjunto de usuarios de un mismo servicio *cloud*, pero no sea accesible directamente por cualquier internauta sino únicamente por otros usuarios, no será necesario invocar el derecho al olvido, sino que será suficiente con que se ejercite el derecho a la supresión, ya que es el mismo proveedor *cloud* que trata los datos quien puede proceder a su eliminación. En el caso en el que sea un empresario quien contrata estos servicios *cloud* para tratar datos de terceros, se entiende que este tratamiento debe realizarse con la máxima seguridad y confidencialidad, y siempre de acuerdo con el consentimiento prestado por el interesado y a las finalidades establecidas; todo ello según el artículo 5 del propio Reglamento, que establece los principios relativos al tratamiento.

Nos congratula que por fin aparezca reconocida legalmente esta facultad del titular, que en reiteradas ocasiones se veía indefenso ante grandes multinacionales de servicios en línea, ya que lo consideramos un mecanismo útil para mitigar los efectos que la difusión de la información puede provocar sobre la persona. Efectos que, por otro lado, tienen un potencial alcance viral o multiplicador si la difusión se realiza a través de la Red u otros medios de comunicación masiva[204].

3.- El derecho a la portabilidad tiene una especial incidencia en el ámbito de

---

remitimos al capítulo "Concepto y características técnicas de la computación en la nube".

203 La sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 en el marco del caso Google Spain contra la Agencia Española de Protección de Datos fue el inicio de la materialización del derecho al olvido en la práctica jurídica de la protección de datos personales, y ha sido finalmente objeto de protección legal específica en el Reglamento General de Protección de Datos. Al respecto, nos remitimos a COBAS COBIELLA, Maria Elena, "Derecho al olvido: de la STJUE de 2014 al Reglamento Europeo de Protección de Datos", *Actualidad Civil,* núm. 1, 2017, págs. 98 a 116; a RALLO LOMBARTE, Artemis, "El debate europeo sobre el derecho al olvido en Internet", *Hacia un nuevo derecho europeo de protección de datos,* Valencia, 2015, págs. 703 a 737; a MINERO ALEJANDRE, Gemma, "A vueltas con el Derecho al Olvido. Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital", *Revista Jurídica de la Universidad Autónoma de Madrid*, núm. 20, 2014, págs. 129 a 155;y a TRONCOSO REIGADA, Antonio, "Las redes sociales a la luz de la propuesta de Reglamento General de Protección de Datos Personales. Parte dos", *Revista d'Internet, Dret i Política*, núm. 16. 2013, págs. 27 a 39.

204 Por ejemplo, problemas de discriminación, usurpaciones de identidad o fraude, daños en la reputación, tal y como reconoce el Considerando 75 del Reglamento General de Protección de Datos.

la computación en la nube[205]. El Grupo de Trabajo del Artículo 29 ya recomendó en el año 2012 que los contratos de servicios de *Cloud Computing* adoptasen formatos de portabilidad estandarizados o abiertos e integrasen cláusulas que estipulasen los formatos y los costes de la migración de datos a otros proveedores, lo cual afectaba del mismo modo a todos los contenidos migrados en general, entendiéndose incluidos en estos contenidos los datos de carácter personal. Asimismo, el Grupo de Trabajo afirmaba que el cliente de servicios de computación en la nube (sin distinguir si ese cliente tenía la consideración de titular de los datos, responsable o encargado del tratamiento) debería asegurarse de las garantías que ofrecía el proveedor en cuanto a la portabilidad de los datos de manera previa a la suscripción del contrato[206]. En su Opinión sobre la adopción del código de conducta C-SIG para proveedores de servicios de *Cloud Computing* y elaborado por representantes de la industria, el Grupo de Trabajo del Artículo 29 animaba a la adopción de estándares referentes a la interoperabilidad, a la portabilidad y a la seguridad de los datos por parte de la industria y sugirió la necesidad de que este código de conducta recoja alguna cláusula que mencione la portabilidad de los datos personales y la exigencia de que los proveedores implementen interfaces que permitan a los clientes-responsables auditar el tratamiento de datos personales encomendado a los proveedores encargados del tratamiento[207].

Con el Reglamento General de Protección de Datos se ha dado reconocimiento legal a esta recomendación. La portabilidad se ha convertido en un nuevo derecho del interesado que le permite recuperar sus datos personales en un formato útil. En su Considerando 68, el Reglamento reconoce la introducción de este nuevo derecho como mecanismo para reforzar el control del interesado sobre sus datos en tratamientos que tienen lugar de forma automatizada y con el fin de

205 Para más detalle, nos remitimos a ROSSELLÓ RUBERT, Francisca Mª, "La recuperación de los contenidos alojados y su portabilidad; en especial, su previsión por el Reglamento 2016/679 General de Protección de Datos de la UE", *Hacia una justicia 2.0, Actas del XX Congreso Iberoamericano de Derecho e Informática* (Dir. Federico Bueno de Mata), Salamanca, 2016, págs. 283 a 298.

206 Dictamen 5/2012 del Grupo de Trabajo del Artículo 29 sobre el *Cloud Computing* [en línea], (WP 196), pág. 16. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>. [Fecha de consulta: 15 de mayo de 2017].

207 GRUPO DE TRABAJO DEL ARTÍCULO 29. *Opinion 2/2015 on C-SIG Code of Conduct on Cloud Computing* [en línea], (WP 232), pág. 11. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf>. [Fecha de consulta: 15 de mayo de 2017].

facilitar la transmisión de esos datos digitales con la máxima facilidad y garantías. El ejercicio del derecho a la portabilidad debe realizarse de manera que los derechos de terceros interesados también queden salvaguardados, ni tampoco debe suponer un obstáculo al ejercicio de los derechos de supresión y limitación del tratamiento.

Recientemente, el Grupo de Trabajo del Artículo 29 ha elaborado unas Directrices expresamente enfocadas en el nuevo derecho a la portabilidad reconocido por el Reglamento europeo[208]. En este texto, se determina que "El nuevo derecho a la portabilidad de los datos tiene por objetivo facultar a los interesados con respecto a sus propios datos personales, ya que aumenta su capacidad de trasladar, copiar o transmitir los datos personales fácilmente de un entorno informático a otro". Asimismo, el Grupo de Trabajo identifica cuales son los elementos de este derecho: el derecho a recibir datos personales que ha procesado un responsable (al cual nosotros hemos denominado derecho de recuperación de los datos personales), y el derecho a transmitir los datos personales de un responsable del tratamiento a otro sin impedimentos (el cual nosotros identificamos como derecho a la portabilidad *strictu sensu*). Para que el interesado pueda ejercitar este derecho a la portabilidad (en un sentido amplio, es decir, incluyendo el derecho a la recuperación y el derecho a la transmisión entre responsables del tratamiento) serán necesarias determinadas herramientas técnicas, con lo cual "deben ofrecer al interesado la opción de descarga directa y al mismo tiempo permitir que los interesados transmitan directamente los datos a otro responsable del tratamiento"[209]. Asimismo, el derecho a la portabilidad no puede perjudicar derechos de terceros[210].

Hemos comentado anteriormente que el artículo 13.2 del Reglamento europeo requiere al responsable del tratamiento que informe al titular de los datos del período durante el cual se conservarán esos datos, o, en su defecto, los criterios que puedan determinar esa retención de datos. El mismo artículo exige al responsable que, en el momento en el que obtenga los datos personales del interesado, le informe de la existencia del derecho a la portabilidad, junto a la información relativa a los derechos de acceso, rectificación, limitación del

208 GRUPO DE TRABAJO DEL ARTÍCULO 29. *Directrices sobre el derecho a la portabilidad de los datos* [en línea], adoptado el 13 de diciembre de 2016. Disponible en: <http://www.agpd.es/portalwebAGPD/internacional/textosynormas/textos_union_europea/textos_articulo_29/common/es_es_wp242_en_40852_PORTABILIDAD.PDF>, pág. 4. [Fecha de consulta: 15 de mayo de 2017].

209 GRUPO DE TRABAJO DEL ARTÍCULO 29. *Directrices sobre el derecho a la portabilidad de los datos, op. cit.*, pág. 5.

210 GRUPO DE TRABAJO DEL ARTÍCULO 29. *Directrices sobre el derecho a la portabilidad de los datos, op. cit.*, pág. 9.

tratamiento y oposición[211]. Además de estas previsiones es en su artículo 20 donde el Reglamento europeo recoge, de forma novedosa, el derecho del titular de los datos personales a la portabilidad de esos datos212. A continuación, pasamos a analizar este artículo 20 y a relacionarlo con los contratos de computación en la nube.

a) Del apartado primero de este artículo 20 puede extraerse que el derecho del interesado se subdivide en tres facultades. La primera de estas facultades consistiría en que el responsable debe entregarle los datos personales facilitados[213]. El artículo 20.1 menciona expresamente que el derecho a la portabilidad debe ejercitarse ante el responsable del tratamiento. En el caso que nos ocupa, es decir, cuando quien ha contratado el servicio *cloud* es un pequeño empresario para utilizarlo en tratamientos de datos de terceros, será el pequeño empresario responsable del tratamiento quien debe gestionar que el interesado pueda recuperar sus datos personales. Como responsable, el empresario deberá exigir al proveedor de servicios *cloud*, en el marco del contrato que vincule a responsable y encargado del

211 El artículo 13.2 del Reglamento General de protección de datos establece: "Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: (...) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; (...)". Ver también GRUPO DE TRABAJO DEL ARTÍCULO 29. *Directrices sobre el derecho a la portabilidad de los datos, op. cit.*, pág. 12.

212 Artículo 20 del Reglamento Reglamento General de Protección de Datos: "El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados. 2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. 3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. 4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros".

213 Como hemos recalcado en diferentes ocasiones en este trabajo, los clientes-empresarios que tratan datos personales de terceros en sistemas del proveedor *cloud* son considerados responsables del tratamiento, siendo los prestadores de servicios *cloud* relegados al rol de encargados, de acuerdo con las manifestaciones que previamente han realizado autoridades competentes en la materia, como la Agencia Española de Protección de Datos o el Grupo de Trabajo del Artículo 29. El proveedor *cloud,* por su parte, será responsable del tratamiento de datos personales ante el titular que contrate directamente sus servicios, y será ante el proveedor cloud quien el interesado suscritor, en este caso, ejercite el derecho a la portabilidad. Ver apartado "La asignación de roles de titular de los datos, responsable y encargado del tratamiento en la computación en la nube", en este mismo capítulo.

tratamiento de datos personales, que le facilite la información necesaria y en el formato pertinente, y en definitiva, la asistencia que requiera el responsable para poder dar cumplimiento a las exigencias legales en relación a la portabilidad de los datos de carácter personal.

b) El artículo 20.2 ofrece al interesado la facultad de que, en la medida en que sea técnicamente posible, el responsable a quien suministró los datos en su momento transfiera los datos al nuevo responsable, exonerando al interesado de esa tarea[214]. Este artículo cobra especial relevancia en aquellos casos en los que la portabilidad de datos pueda tener lugar entre proveedores de computación en la nube o profesionales informáticos.

Sin embargo, cuando el responsable del tratamiento sea un empresario cuya actividad económica no esté relacionada con la técnica informática, puede tener dificultades para facilitar los datos a otro empresario, debido a la falta de conocimientos técnicos o de infraestructura apropiada. Cuando se ponga de relieve tal dificultad práctica vinculada a los conocimientos y recursos del responsable, este retornará los datos al interesado directamente, en un "formato útil, de uso común y lectura mecánica", puesto que con estos requisitos habrá exigido el retorno de los datos al proveedor *cloud* encargado el tratamiento, para que sea el propio interesado quien los facilite a quien ocupe a partir de ese momento la posición de responsable del tratamiento. No obstante, el hecho de que el responsable del tratamiento no disponga de los mecanismos técnicos adecuados para facilitar la transmisión de los datos personales a otro proveedor no puede servir de argumento para dejar al derecho a la portabilidad vacío de contenido, sino que siempre deberá facilitar en la medida de sus posibilidades la transmisión de esos datos al nuevo responsable o su devolución al interesado en un formato que le permita transferirlos de manera sencilla y sin necesidad de volver a reintroducirlos.

Por otra parte, como se ha dicho, el derecho a la portabilidad deberá respetar en todo caso los derechos de terceros, lo cual puede ser relevante en entornos compartidos de nube pública en los cuales los mismos soportes físicos o aplicaciones pueden servir para el tratamiento de datos personales de numerosos ciudadanos. En

214 Ya en su Considerando 68, el Reglamento General de Protección de Datos establece que "Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. (...) El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. (...) . El interesado debe tener derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible".

estos casos, será el proveedor *cloud* quien se asegure de que el ejercicio de derechos de un interesado no afecte a los datos o derechos de otros.

c) Junto a la facultad de recuperar los datos, el artículo 20.1 permite al interesado exigir que esos datos personales le sean devueltos en un formato estructurado, de uso común y lectura mecánica. El sentido de la expresión "formato estructurado" no se define en el Reglamento europeo, aunque parece que cobra sentido como descriptor de aspectos referentes a la técnica de codificación del archivo o archivos que contendrán los datos personales. Los contenidos presentados en formatos estructurados pueden ser fácilmente importados y procesados por diferentes sistemas informáticos, y pueden sujetarse a ciertos estándares. En cuanto a la exigencia de "uso común" y "lectura mecánica", entendemos que estas expresiones exigen, respectivamente, que el formato en el cual se retornen los datos pertenezca a tecnologías ampliamente utilizadas y reconocibles, para que esos datos puedan ser incorporados a otros sistemas informáticos que permitan proseguir con su tratamiento automatizado. Estas características no se definen ni por el Reglamento europeo ni por las Directrices del Grupo de Trabajo del Artículo 29[215], aunque este último afirma que "Los términos «estructurado», «de uso común» y «legible por máquina» son un conjunto de requisitos mínimos que deben facilitar la interoperabilidad del formato de datos proporcionado por el responsable del tratamiento. En ese sentido, «estructurado, de uso común y legible por máquina» son especificaciones para los medios, mientras que la interoperabilidad es el resultado deseado". El Considerando 68 del Reglamento europeo aclara que el formato debe ser interoperable (entendiendo la interoperabilidad como "la capacidad de que organizaciones dispares y diversas actúen en pos de objetivos comunes mutuamente beneficiosos y acordados, en relación con la puesta en común de información y conocimiento entre las organizaciones, a través de los procesos empresariales que respaldan, mediante el intercambio de datos entre sus sistemas de TIC respectivos"[216]) y que ello no implica que los los sistemas de tratamiento entre responsables del tratamiento deban ser compatibles entre sí ("El derecho del interesado a transmitir o recibir datos personales que le incumben no debe crear la obligación para los responsables del tratamiento de adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles"). Además, el Grupo de Trabajo interpreta que "Los responsables del tratamiento deben proporcionar junto con los datos tantos metadatos como sea posible con el mejor nivel posible de granularidad, que preserve el significado exacto de la información intercambiada", con

215 GRUPO DE TRABAJO DEL ARTÍCULO 29. *Directrices sobre el derecho a la portabilidad de los datos, op. cit.*, pág. 14.

216 Esta definición viene dada por la Decisión núm. 922/2009/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 relativa a las soluciones de interoperabilidad para las administraciones públicas europeas (pág. 20). GRUPO DE TRABAJO DEL ARTÍCULO 29. *Directrices sobre el derecho a la portabilidad de los datos, op. cit.*, pág. 13.

el fin de facilitar al máximo la reutilización de esos datos[217].

d) El apartado tercero del artículo 20 dispone que el derecho a la portabilidad se conjugará con el derecho a la supresión definitiva de los datos personales (es decir, con el borrado de datos) una vez que tales datos ya no sean necesarios para la ejecución del contrato entre el titular de los datos y el responsable. Por su parte, el Grupo de Trabajo del Artículo 29 desvincula el derecho a la portabilidad con el borrado de los datos personales ("La portabilidad de los datos no conlleva automáticamente el borrado de los datos de los sistemas del responsable del tratamiento ni afecta al periodo de retención original aplicable a los datos que se han transmitido"), y con la extinción de cualquier relación contractual ("Un interesado puede seguir usando y beneficiándose del servicio del responsable del tratamiento incluso después de una operación de portabilidad de datos")[218].

En la práctica, aunque el responsable del tratamiento de datos personales es quien debe garantizar al titular de los datos la recuperación y, en su caso, el posterior borrado efectivo de los sistemas, el empresario suscriptor de servicios de computación en la nube no siempre tiene a su alcance los conocimientos técnicos o la infraestructura adecuada para permitir un ejercicio eficiente del derecho al borrado efectivo de los datos, con lo cual deberá, como responsable del tratamiento, elegir un proveedor *cloud* que ponga a su disposición las herramientas suficientes para conseguir que la migración de datos personales a entornos de nube no sea un obstáculo en el ejercicio de los derechos del interesado, entre ellos el derecho a la supresión de los datos personales[219].

Como valoración general de este precepto, consideramos que el artículo 20 del Reglamento supone un paso hacia adelante en el reconocimiento del derecho a la portabilidad de los datos personales por parte de los interesados titulares de esos datos. Consideramos que el Grupo de Trabajo ha aclarado algunas dudas sobre el ejercicio del derecho a la portabilidad, siendo una de las afirmaciones más relevantes la desvinculación de este derecho con la extinción del contrato entre titular de los datos y el responsable del tratamiento. Sería recomendable, a nuestro parecer, que

217 Esta definición viene dada por la Decisión núm. 922/2009/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 relativa a las soluciones de interoperabilidad para las administraciones públicas europeas (pág. 20). GRUPO DE TRABAJO DEL ARTÍCULO 29. *Directrices sobre el derecho a la portabilidad de los datos, op. cit.*, pág. 13.

218 GRUPO DE TRABAJO DEL ARTÍCULO 29. *Directrices sobre el derecho a la portabilidad de los datos, op. cit.*, pág. 6.

219 Ver apartado "Los efectos de la finalización del contrato de computación en la nube sobre los datos personales".

este reconocimiento se hiciese extensible, en un futuro no muy lejano, a otros intermediarios que puedan beneficiarse de la portabilidad de datos personales, además de los interesados. Sería, por ejemplo, el caso del empresario suscriptor de servicios de computación en la nube, responsable del tratamiento, que tiene la iniciativa de cambiar de proveedor *cloud* (es decir, de encargado del tratamiento) para proseguir con las herramientas informáticas del nuevo encargado la tarea del procesamiento de datos personales de terceros.

Aun así, nosotros entendemos que, aunque el derecho legal a la portabilidad se predique únicamente del titular de datos personales, el empresario que trate datos en la nube, en su papel de responsable del tratamiento, puede exigir del proveedor en la nube la portabilidad de los datos personales de terceros que quedan bajo su tutela, y que el proveedor *cloud* deberá seguir sus instrucciones en cumplimiento de su posición jurídica de encargado, pues así se comprometió en el contrato exigido legalmente a tal efecto entre responsable y encargado (art. 12 LOPD) y entre importador y exportador de datos personales en transferencias internacionales.

Queremos puntualizar que, aunque aplaudimos la iniciativa de recoger el derecho a la recuperación y portabilidad de datos personales en el Reglamento General de Protección de Datos, no existe en la actualidad obligación legal que garantice la portabilidad de los datos de carácter no personal. Aunque la Propuesta de Directiva de Suministro de Contenidos Digitales prevé la devolución al consumidor de todos los contenidos facilitados mediante el uso de servicios de suministro de contenidos digitales, como veremos en posteriores capítulos, quedan todavía carentes de protección legal aquellos contenidos migrados por empresarios, y especialmente indefensos los pequeños empresarios sin facultad para negociar el contrato *cloud*[220].

Consideramos, al respecto, que el proveedor *cloud,* en cumplimiento de su deber de diligencia, debería informar antes de suscribir el servicio si existe o no la posibilidad de que el usuario (empresario o particular) recupere sus datos en un formato que le sea útil, el procedimiento mediante el cual se llevará a cabo, si tendrá o no asistencia, y los costes de la recuperación. Igualmente, animamos a la incorporación de un derecho amplio de recuperación y portabilidad, que abarque contenidos migrados por cualquier cliente, sea cual sea la naturaleza de estos datos.

220 Ver capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

Lo anterior se desprende de la propia naturaleza del contrato de servicios de computación en la nube pública.

Ante la inexistencia de reconocimiento legal del derecho a la portabilidad de (todos) los datos migrados a entornos de nube, el Grupo de Expertos de la *Cloud Computing Strategy* ha planteado diferentes soluciones[221]. Entre estas ideas, destaca la adopción de cláusulas modelo para contratos de computación en la nube, implementadas por la industria, y que sean comprensibles, transparentes y con una eficaz aplicación práctica[222]. Aunque variarán según el modelo de implementación de nube, sería aconsejable que incluyesen, según los propios expertos: una definición de "datos" o "contenidos", la identificación de aquellos datos que pueden exportarse o recuperarse; el formato en el cual se pueden recuperar (por ejemplo, sugieren un formato estándar) y, por tanto, que sean portables a otras nubes; si el retorno tiene o no un coste añadido, y que, en caso de existir, que sea razonable; durante qué plazo, una vez terminado el contrato, el proveedor se compromete a preservar los datos; y que los datos no pueden ser borrados mientras esté pendiente la resolución de un conflicto entre las partes, excepto que sea el propio cliente quien exija tal borrado[223].

221 CLOUD COMPUTING STRATEGY, *Discussion Paper on Switching- Data Portability upon switching* [en línea], 2014. Disponible en: <http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_topic_4_switching_en.pdf>. [Fecha de consulta: 31 de agosto de 2016].

222 En pro de la transparencia, el Grupo de Expertos de la *Cloud Computing Strategy* propone un conjunto de iconos que indican cuando un usuario puede transferir los metadatos, si pueden migrarse los datos a otro proveedor, o si la recuperación de los datos depende de un pago añadido. Sin embargo, este mecanismo debe combinarse con la adopción de estándares técnicos que permitan afirmar que los datos migrados son susceptibles de ser portables, tal y como también afirman las Directrices sobre el derecho a la portabilidad, del Grupo de Trabajo del Artículo 29.

223 Así, reconoce el Grupo de Expertos de la *Cloud Computing Strategy* que existen diferencias entre los diferentes servicios *cloud* que pueden afectar a la portabilidad de los datos. El software como servicio (SaaS) implica que el cliente substituye una aplicación por otra, con lo cual es esencial asegurar la funcionalidad que permite la nueva aplicación con los datos transferidos por el primer proveedor. Cuando se trata de plataformas como servicio (PaaS), debe ponerse el punto de mira en minimizar la cantidad de aplicación que debe reescribirse, porque además de datos y metadatos, será necesario transferir códigos base y marcos de desarrollo de aplicaciones. En servicios de infraestructura (IaaS), lo esencial será la configuración de las infraestructuras entre los proveedores *cloud* entrante y saliente, y la capacidad de portar máquinas virtuales y sus configuraciones subyacentes.

4.-LOCALIZACIÓN Y SEGURIDAD DE LOS DATOS. ACCESO A DATOS POR TERCEROS, CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES

En las transferencias internacionales de datos personales que tienen lugar en el marco de relaciones de computación en la nube existe un flujo constante de datos entre diferentes centros de procesamiento. Los datos están localizados en ubicaciones múltiples, dispares y simultáneas, con lo cual lo habitual es que el responsable del tratamiento desconozca la ubicación de los datos, en qué lugar o lugares están almacenados o replicados, y a qué destinos están siendo transferidos en cada momento[224].

Debido a las particularidades del funcionamiento de la computación remota, la regulación de la Directiva 95/46 y de nuestras normas de transposición resulta rígida y poco flexible en su aplicación al contexto *cloud*, ya que, evidentemente, este contexto no fue tomado en consideración al regularse originariamente el marco legal. La Comisión Europea ha tratado de solventar las trabas burocráticas en esta materia mediante decisiones que consideran la aptitud de ciertos destinos de datos personales en cuanto a un tratamiento garante de los derechos de los interesados europeos, algunas veces con más acierto que otras (como constató en su momento la anulación de la Decisión relativa al *Safe Harbor* por el Tribunal de Justicia de la Unión Europea[225]).

A continuación, dedicaremos este apartado a la regulación de las transferencias internacionales de datos de carácter personal, tanto en el contexto general como en el marco de transferencias derivadas de servicios de computación en la nube, y analizaremos los instrumentos jurídicos a disposición de los actores involucrados en la transferencia para garantizar el cumplimiento de la normativa europea y nacional. Nos referiremos asimismo lo establecido al respecto por el Reglamento General de Protección de Datos.

224 PUYOL MONTERO, Javier; *Algunas consideraciones..., op. cit.*, págs. 154, 155.

225 Al respecto, nos remitimos a ROSSELLÓ RUBERT, Francisca Mª; "La transferencia de datos personales entre PYME españolas y proveedores norteamericanos de *Cloud Computing* tras la reciente anulación del Acuerdo *Safe Harbor* por el Tribunal de Justicia de la Unión Europea", *Diario La Ley*, núm. 8725, 2016.

4.1.- Localización física de los datos

En los contratos entre cliente y proveedor de computación en la nube no siempre se encuentra información sobre la localización física de los datos personales dentro de la infraestructura del proveedor[226]. Algunos grandes proveedores se comprometen por vía contractual a mantener los datos de sus clientes dentro de centros de procesamiento ubicados en determinadas "zonas regionales", restringiendo de este modo la transferencia a países que queden fuera de estas zonas[227]. Otros, sin embargo, no mencionan los lugares de posible ubicación de los datos[228].

Exista o no previsión contractual, la realidad es que el responsable

226 Cuando el proveedor facilita información sobre la localización física de estos datos, puede entenderse como un compromiso contractual que debe cumplir, parte integrante del acuerdo de nivel de servicio (ANS), y a modo de Objetivo de Nivel de Servicio (ONS). Ver apartado "Descripción técnica del acuerdo de nivel de servicio (ANS) y sus parámetros: los objetivos de nivel de servicio (ONS)", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

227 Por ejemplo, el servicio de *Amazon Web Services S3* (*Simple Storage Services*), dedicado al almacenamiento de datos (en especial para empresas y profesionales TIC que desarrollen aplicaciones en la nube, distribuyan contenidos o utilicen herramientas de análisis de *Big Data*), permite al suscriptor elegir una región, dentro de la cual los datos se almacenarán de forma redundante en diferentes dispositivos de instalaciones que se encuentran allí localizadas, y desde donde serán accesibles. Los criterios de elección de la región por el cliente pueden basarse en el cumplimiento de requisitos legales, pero también en otros motivos como la reducción de la latencia de acceso a los datos, la consecución de redundancia geográfica que le garantice la recuperación de los datos, o la reducción de costes, dado que algunas zonas son más económicas que otras. En su sitio web se ofrece información sobre las regiones en su sección "Preguntas Más Frecuentes", y el contrato lo recoge en su cláusula 3.2 [en línea]. Disponible en: <https://aws.amazon.com/es/s3/faqs/>; y <http://aws.amazon.com/es/agreement/>. [Fecha de consulta: 15 de mayo de 2017].

228 Aunque Google permita, a través de su web, visitar virtualmente algunos de sus centros de datos, su política de privacidad no menciona las diferentes localizaciones físicas en las cuales pueden almacenarse y replicarse los datos de los ciudadanos europeos. Disponible en: <http://www.google.com/intl/es-419/about/datacenters/gallery/#/>; y <http://www.google.es/intl/es/policies/privacy/#products>. [Fecha de consulta: 15 de mayo de 2017]. Lo anterior no significa que Google no cumpla con las garantías legales necesarias para la transferencia internacional de datos. De hecho, el 30 de agosto de 2016, los servicios de nube *Google Apps* (ahora *Google G-Suite*) y *Google Cloud Platform* se adhirieron al marco de protección de datos *Shield*, un acuerdo de colaboración entre el Departamento de Comercio norteamericano y la Unión Europea para el cumplimiento de la normativa europea que se transfiere a EE.UU, del cual hablaremos más adelante. Más información disponible en los sitios web oficiales del *Privacy Shield* y de Google: <https://www.privacyshield.gov/welcome> y <http://googleforwork.blogspot.com.es/2016/08/Google-adopts-Privacy-Shield.html?m=1>. [Fecha de consulta: 15 de mayo de 2017].

difícilmente puede conocer la ubicación de sus datos a tiempo real, ni cuantas copias o transferencias de información sensible pueden estar llevándose a cabo, con lo cual existe el riesgo de que los datos acaben en países de destino con un nivel de protección de datos inferior al europeo[229]. La verificación del lugar donde efectivamente se están procesando los datos resulta técnicamente compleja.

No obstante, en opinión de los expertos de la *Cloud Computing Strategy,* el principal problema no radica tanto en conocer su ubicación exacta[230], sino en saber quién puede tener acceso a los datos (en principio, solo el responsable y aquellos encargados o subencargados autorizados por aquel), las garantías y riesgos que ofrece el proceso de transmisión o tránsito[231]; y la legislación aplicable y las autoridades que puedan acceder a esos datos[232]. Debemos ser conscientes de que es el proveedor quien tiene la capacidad y el poder de decisión en cuanto a la provisión de la seguridad de sus propias instalaciones, sistemas y conexiones de red.

Sin embargo, cuando no existe previsión contractual sobre la localización de los datos, el suscriptor empresario responsable del tratamiento debe poder averiguar dónde, cuándo y quién ha almacenado o procesado los datos personales bajo su tutela dentro de la cadena de recursos del proveedor, y en qué condiciones de seguridad. En caso contrario, como afirma la Agencia Española de Protección de Datos, nos encontraremos ante un servicio opaco, carente de transparencia y que no permite al usuario auditar y controlar la información[233].

---

229 ALAMILLO DOMINGO, Ignacio, "El control de localización de los datos e informaciones en el Cloud", en *Derecho y Cloud Computing* (coord. Ricard Martínez Martínez), Navarra, 2012, pág. 72.

230 Por otra parte, proporcionar al detalle ubicaciones exactas puede redundar en riesgos en la seguridad de los sistemas físicos de los proveedores, haciéndolos más susceptibles a ataques. Por otro lado, la flexibilidad del proveedor para mover y replicar los datos coadyuva a las mayores ventajas en cuanto a precio, disponibilidad y resiliencia de los servicios computación en la nube.

231 La política de privacidad de Apple asegura al cliente que la empresa "se toma muy en serio la seguridad de su información personal. Los servicios *online* de Apple, como *Apple Online Store* y *iTunes Store*, protegen su información personal durante el tránsito con métodos de cifrado, como *Transport Layer Security* (TLS). Cuando Apple almacena sus datos personales, usamos sistemas informáticos con acceso restringido alojados en instalaciones que usan medidas de seguridad física. Los datos de *iCloud* se almacenan cifrados, incluso cuando usamos almacenamiento de terceros". Disponibles en: <http://www.apple.com/mx/privacy/privacy-policy/>. [Fecha de consulta: 15 de mayo de 2017].

232 Así lo afirma el Grupo de Expertos en su *Discussion paper on Data Location and Security,* de marzo de 2014, y en su *Discusion Paper Topics to be Covered by the Experts Group* [ambos documentos en línea], de noviembre de 2013. Disponibles en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 15 de mayo de 2017].

233 AEPD, *Guía para clientes que contraten servicios de Cloud Computing* [en línea], pág. 10.

Consecuentemente, esta falta de información choca con la obligación del cliente empresario, como responsable del tratamiento, de impedir la transferencia de datos a aquellos países fuera del Espacio Económico Europeo que no cumplan con los requisitos legales comunitarios. Como veremos más adelante, tanto los arts. 25 y 26 de la Directiva 95/46/C como los artículos 44 a 50 del Reglamento General de Protección de Datos permiten la transferencia internacional de datos personales a países fuera del EEE únicamente cuando el país importador garantice un nivel adecuado de protección de datos[234]. Asimismo, los contratos suscritos por el proveedor con subproveedores deben seguir manteniendo la protección de datos acordada, puesto que el acceso a datos de usuarios por subcontratistas de otros países puede implicar igualmente una transferencia internacional.

4.2.- Transferencias internacionales de datos y *Cloud Computing*

La Directiva 95/46/CE no define la transferencia internacional[235]. Tampoco el nuevo Reglamento General de Protección de Datos define este concepto[236]. A falta de definición en la normativa comunitaria, podemos tomar como referencia la definición de transferencia internacional de datos personales recogida en el art. 5.1.s) RLOPD: "tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español".

4.2.1.- Concepto de transferencia internacional de datos de carácter personal

De acuerdo con la normativa aplicable actualmente (LOPD y RLOPD), en las

---

Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf>. [Fecha de consulta: 15 de mayo de 2017].

234 Ver apartado "Transferencias internacionales de datos y *Cloud Computing*", en este mismo capítulo.

235 Es importante destacar que las transmisiones de datos dentro del Espacio Económico Europeo se consideran una cesión de datos, no serán consideradas transferencia internacional y, por consiguiente, no será necesario que cumplan con todos los requisitos legales de estas.

236 Sí recoge, en cambio, la definición de "tratamiento transfronterizo", como "a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro", en su artículo 4.23.

transferencias internacionales, el exportador de datos[237] sujeto a la LOPD transmite información de carácter personal al importador de datos[238] de un tercer país, ya sea para que este los trate como responsable fuera del Espacio Económico Europeo, ya sea para que los trate por cuenta del responsable fuera del Espacio Económico Europeo. Como observamos, implica una salida física de los datos fuera del Espacio Económico Europeo.

Las transferencias internacionales deben ser consentidas por el titular de los datos, quien autorizará al responsable para efectuarlas[239]. Sin embargo, la obtención de este consentimiento en el marco de la computación en la nube presenta algunos problemas, entre los cuales destacan el elevado número de titulares de datos personales, los propósitos del tratamiento no siempre transparentes o la múltiple ubicación de los datos[240].

4.2.2.- Diferencias en las garantías exigidas a las transferencias internacionales, atendiendo al país receptor de los datos personales

Será esencial determinar el establecimiento del proveedor de servicios *cloud* para identificar el país importador de datos personales de ciudadanos europeos. Así, las transferencias internacionales pueden tener ser, según la normativa aplicable en la actualidad:

1.- Transferencias internacionales a países importadores con nivel adecuado de protección de datos. Entre estos países se encuentran

a) Países que forman parte del EEE[241]. A ojos de la normativa, estas cesiones de datos se consideran meras comunicaciones de datos y, por tanto, quedan

237 El concepto de exportador de datos aparece definido en el art. 5.1.j) RLOPD como "la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero".

238 El concepto de importador se recoge en el art. 5.1.ñ) RLOPD: "la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero".

239 Ver apartado "El titular de los datos y la prestación de consentimiento informado e inequívoco", en este mismo capítulo.

240 Así lo manifiestan el Grupo de Expertos de la *Cloud Computing Strategy,* en su *Discussion Paper on Data Transfers in the Cloud* [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_data_transfers_in_cloud.pdf>. [Fecha de consulta: 15 de mayo de 2017].

241 El Espacio Económico Europeo integra todos los Estados miembros de la UE e Islandia, Liechtenstein y Noruega.

exentas de los requisitos de las transferencias internacionales al ofrecer una protección ya no adecuada, sino equivalente a la LOPD[242];

b) Países que han recibido la aprobación de la Comisión Europea[243], que de acuerdo con el art. 34.k) de la LOPD y 68 del RLOPD quedan eximidos de la exigencia de la autorización por parte de la Agencia Española de Protección de Datos.

En el caso de EE. UU, cabe destacar que la Comisión únicamente reconocía el nivel adecuado de protección a aquellas empresas y entidades acogidas a los principios de puerto seguro o *Safe Harbor*[244]. Se trataba, como veremos en un apartado *ad hoc*, de un acuerdo transatlántico que consideraba que tales destinos presentaban un "sistema de garantías adecuado", acuerdo que fue anulado por el Tribunal de Justicia de la Unión Europea, y que fue substituido por el denominado acuerdo *Shield*, cuyas medidas de protección son más reforzadas[245].

---

242 El acceso por cuenta de terceros, del artículo 12 LOPD, regula la posibilidad de que el responsable permita a un tercero (que se posicionará jurídicamente como encargado), trate los datos por cuenta del responsable. este encargado está obligado a seguir estrictamente sus instrucciones y a devolver o destruir los datos una vez haya finalizado el servicio (art. 12.3 LOPD), y su relación con el responsable se regirá por el contrato que debe existir entre ambos de acuerdo con el artículo 12.2 LOPD, y además, por los artículos 20 a 23 del RLOPD. El nuevo Reglamento General de Protección de Datos no recoge el término "cesión" o "comunicación de datos" en el mismo sentido de la LOPD, aunque sí se recoge el deber de información del responsable al interesado sobre los destinatarios de datos personales (art. 13.1.e del Reglamento europeo) y se distingue la información que el responsable, salvo algunas excepciones, debe facilitar al interesado en aquellos casos en los que los datos no provengan directamente del propio interesado, sino de otro responsable o encargado (art. 14 del Reglamento europeo).

243 Según la Comisión, los siguientes países ofrecen un nivel adecuado de protección en toda su normativa: Suiza, Argentina, Guernesey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, y el Principado de Mónaco. En el caso de EE. UU y Canadá, únicamente en ciertos casos.

244 Los principios de puerto seguro eran siete principios, publicados en el DOCE L 215 de 25 de agosto de 2000: notificación, opción, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación. Junto a su publicación, también se publicó la Decisión de la Comisión 2000/520/CE sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada. Además, la UE reconoció la competencia de la Comisión Federal de Comercio (*Federal Trade Comission)* y al Departamento de Transporte norteamericanos para investigar prácticas desleales fraudulentas en la aplicación de estos principios, y adoptar medidas provisionales. Medidas que el Tribunal Europeo consideró insuficientes.

245 En el caso de Canadá, únicamente se reconoce el nivel adecuado de protección a los obligados por la *Personal Information and Electronic Documents Act*. Según su Opinión 2/2001 sobre el nivel adecuado de protección de la ley canadiense *Personal Information and Electronic Documents Act,* el Grupo de Trabajo del Artículo 29 cree que la consideración de la normativa

Como podemos observar, la gran mayoría de países no han obtenido este reconocimiento por parte de la Unión Europea, ni tampoco se prevé, en opinión de algunos expertos, que a medio plazo esta lista aumente considerablemente[246]. La adecuación o no del nivel de protección del país de destino de los datos se evaluará por la Agencia Española de Protección de Datos, que tendrá en cuenta los criterios recogidos en el art. 33.2 LOPD[247]. Este requisito puede quedar excepcionado en ciertos casos enumerados por el art. 34 de la LOPD[248].

Apunta el Grupo de Trabajo del Artículo 29 en su informe sobre transferencias internacionales que, para considerar si un país ofrece o no una protección adecuada, será necesario tener en cuenta dos factores: el contenido de las normas reguladoras de la privacidad y los medios que garanticen una aplicación eficaz[249]. Además, elabora una lista de principios mínimos que deben recoger las

---

canadiense como adecuada también es susceptible de mejoras.

246 GUASCH PORTAS, "La transferencia internacional de datos de carácter personal", *Revista de Derecho UNED*, núm. 11. 2012, págs. 413 a 453.

247 Art. 33.2 LOPD. "El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países". Este artículo transcribe casi literalmente el art. 25.2 de la Directiva 95/46/CE.

248 Art. 34 LOPD. "Lo dispuesto en el artículo anterior no será de aplicación: a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España. b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional. c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios. d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica. e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista. f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado. g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero. h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias. i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo. k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado".

249 GRUPO DE TRABAJO DEL ARTÍCULO 29, "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva 95/46 sobre Protección de Datos de la UE" (WP 12), 1998 [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_es.pdf>. [Fecha de consulta: 5 de septiembre de 2016].

normativas de los terceros países para ser considerados garantes del nivel de protección adecuado, y, en su defecto, las soluciones contractuales que pretendan subsanar tales deficiencias y permitan la transferencia a estos países de datos de ciudadanos europeos[250].

2.- Transferencias internacionales a países importadores sin nivel adecuado de protección de datos. En la normativa española se exige, para la transferencia internacional lícita de datos de carácter personal a países sin el nivel adecuado de protección, la formalización del contrato y un autorización de la Agencia Española de Protección de Datos (art. 33.1 LOPD y 66.1 del RLOPD)[251].

El art. 70 del RLOPD indica cómo puede el exportador aportar garantías a un tercer país cuyo nivel de protección no se ha considerado suficiente. Las cláusulas cumplen la función de contrarrestar, con sus efectos vinculantes entre las partes contractuales, la falta de una normativa suficientemente protectora de la privacidad en el país receptor, incluyendo los elementos esenciales para conseguir el amparo del titular de los datos y los efectos prácticos equivalentes a la cobertura legal que ofrece la Directiva. La presentación de estas garantías, las cuales pasamos a enumerar a continuación, se enmarca en el procedimiento establecido por los artículos 137 a 140 del RLOPD, en el marco de la autorización singular del Director de la AEPD para

250 El GT29, en su Documento de Trabajo "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", enumera los siguientes principios básicos de protección de datos: 1.- Principio de limitación de objetivos; 2.- Principio de proporcionalidad y de calidad de los datos; 3.- Principio de transparencia; 4.- Principio de seguridad; 5.- Derecho de acceso, rectificación y oposición; y 6.- Restricciones respecto a transferencias sucesivas a personas ajenas al contrato. También considera la aplicación de otros principios adicionales, relativos a los datos sensibles, a la mercadotecnia directa y a las decisiones automatizadas.

251 La LOPD (art. 33.1) transpone el art. 25.1 de la Directiva 95/46/CE, que dice que "Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado". El art. 26.2 de la Directiva lo complementa, y establece que "los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas". El desarrollo del RLOPD, en su art. 66.1, determina que "será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del propio Reglamento".

transferencias internacionales[252].

a).- Cuando el responsable del tratamiento aporte un contrato escrito entre exportador e importador en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos. La Comisión Europea elaboró unas cláusulas contractuales tipo para facilitar a los responsables la transferencia internacional de datos, que también han sido objeto de estudio por el Grupo de Trabajo del Artículo 29[253].

- Cláusulas tipo entre responsables de tratamiento: para los casos en los que el exportador esté establecido en el EEE y el importador fuera del EEE, en un país sin nivel adecuado de protección. En este caso, el responsable importador de datos no actúa por cuenta del primer responsable, y por tanto, las exigencias son mayores. Existen dos conjuntos de cláusulas tipo: las recogidas por la Decisión 2001/497/CE, de 15 de junio de 2001[254], y las alternativas a estas, recogidas por la Decisión 2004/915/CE (que modifica la decisión anterior) tras

252 Este procedimiento para la autorización de transferencias internacionales de datos a países terceros exige al exportador la aportación de: "a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos. b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica. c) La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso. Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes".

253 A continuación, recogemos las opiniones del Grupo de Trabajo del Artículo 29 relacionadas con las cláusulas contractuales tipo de la UE: "Dictamen 1/2001 sobre el proyecto de Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países al amparo del apartado 4 del artículo 26 de la Directiva 95/46"; "Dictamen 7/2001 relativo al proyecto de Decisión de la Comisión sobre las cláusulas contractuales tipo para la transferencia de datos personales a encargados del tratamiento establecidos en terceros países, al amparo de lo dispuesto en el apartado 4 del artículo 26 de la Directiva 95/46", "Dictamen 8/2003 sobre el proyecto de cláusulas tipo presentado por un grupo de asociaciones empresariales (*The alternative model contract*)"; y el "Dictamen 3/2009 sobre el proyecto de Decisión de la Comisión 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 (de los responsables a los encargados del tratamiento)".

254 Decisión 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE [en línea]. Disponible en: <https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/Dec_2004_915_CE_271204_vers_consoli.pdf>. [Fecha de consulta: 5 de septiembre de 2016].

considerar las propuestas efectuadas por asociaciones empresariales. Ambas decisiones contienen un conjunto de cláusulas modelo que pueden adoptar los responsables del tratamiento, pero no pueden modificarlas o combinar elementos entre los dos conjuntos.

- Cláusulas tipo entre responsable (exportador establecido en el EEE) y encargado (establecido en un país sin el nivel adecuado de protección), y de este encargado a un eventual subencargado (también de un tercer país). Como hemos mencionado, se considera, como norma general, al cliente *cloud* como responsable del tratamiento (y, por ende, sujeto a las obligaciones de la Directiva 95/46/CE); al proveedor *cloud* como encargado y a los eventuales subcontratistas del proveedor como subencargados. Por tanto, estas cláusulas serán una herramienta que permita ofrecer garantías para muchas transferencias internacionales de datos personales derivadas de la prestación de servicios de computación en la nube. Se considerará que presentan las garantías adecuadas aquellos contratos de acceso a datos que incluyan las cláusulas modelo de la Decisión de la Comisión 2010/87, de 5 de febrero de 2010. No obstante, para validar las eventuales transferencias mediante estas cláusulas, es preceptivo que tanto encargado como subencargado estén establecidos en un tercer país fuera del EEE. Las autoridades de control nacionales, además, pueden conceder sus propias autorizaciones, cuando cumplan con la aplicación del art. 26.2 de la Directiva y de sus transposiciones en los ordenamientos nacionales, pero no pueden negarse a reconocer que las cláusulas tipo de la Decisión 2010/87/CE proporcionan las garantías adecuadas.

- Cláusulas tipo entre encargado establecido en el EEE (autorizado previamente por responsable establecido en el EEE) y subencargado establecido fuera del EEE. Las cláusulas de la AEPD adoptadas en su resolución de transferencia internacional de datos de 16 de octubre de 2012[255] solventan el vacío normativo de transferencias internacionales

255 Modelo de cláusulas contractuales de la AEPD para encargado establecido en España y subencargado de tercer país sin nivel adecuado de protección [en línea], basadas en el Considerando 23 de la Decisión 2010/87/UE, que permite a las autoridades nacionales flexibilizar la subcontratación entre encargados nacionales y subencargados de países sin nivel de protección adecuado. Disponible en:

de datos entre un encargado establecido en España y un subencargado de un tercer país que no garantiza el nivel adecuado de protección[256]. Además de este contrato, debe aportarse el contrato marco entre el responsable del tratamiento y el encargado, donde se refleje la autorización del responsable en materia de transferencia internacional de datos y subcontratación. En el contrato se describirán los servicios prestados por el subencargado, la descripción de finalidades y categorías de datos objeto de tratamiento así como la descripción de las medidas de seguridad que va a aplicar el subencargado. Nuestra AEPD fue pionera, dentro de las autoridades de control, en la redacción de este tipo de cláusulas, y el Grupo de Expertos de la *Cloud Comuting Strategy* las consideró un buen modelo a seguir para las demás autoridades de control[257]. El Grupo de Trabajo del Artículo 29 redactó en 2014, un borrador con cláusulas para transferencias entre encargados del tratamiento establecidos en el EEE y subencargados establecidos en terceros países sin un nivel de protección adecuado[258]. Estas cláusulas no constituyen un nuevo conjunto equiparable, en términos de seguridad jurídica, al ofrecido por la Comisión Europea, y por tanto no pueden sustituirlas asumiendo que se obtienen plenas garantías de acuerdo con el art. 26.2 de la Directiva 95/46/CE, pero sí

<https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/common/pdfs/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf>. [Fecha de consulta: 5 de septiembre de 2016].

256 Mientras no se adopte ningún instrumento específico para este caso, el Grupo de Trabajo del Artículo 29 en su "Documento sobre preguntas más frecuentes para aclarar algunas cuestiones en relación con la Decisión 2010/87/UE (WP 176)" [en línea] considera, en su pregunta tercera, tres posibles soluciones: en primer lugar, la redacción de un contrato entre el responsable de tratamiento y el subencargado establecido fuera del EEE, conforme a la Decisión 2010/87/UE; en segundo lugar, un mandato expreso del responsable que permita al encargado fuera del EEE la utilización de las cláusulas tipo de la Decisión 2010/87/CE para subcontratar, siempre dentro del tratamiento acordado; y por último, un contrato *ad hoc*, de acuerdo con el Considerando 23 de la Decisión 2010/87/UE. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp176_en.pdf>. [Fecha de consulta: 5 de septiembre de 2016].

257 Así lo afirma en su *Discussion Paper on Data Transfers in the Cloud,* publicado en 2014 [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 5 de septiembre de 2016].

258 Se trata del Documento de Trabajo " *Working Document 01/2014 on draft ad hoc contractual clauses EU data procesor to non-EU sub-processor* (WP 214) [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_data_transfers_in_cloud.pdf>. [Fecha de consulta: 5 de septiembre de 2016].

pueden contribuir a la autorización de transferencias por parte de autoridades nacionales que carecen de cláusulas propias.

b).- Cuando, dentro de grupos empresariales multinacionales, se adopten reglas internas de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la LOPD y el propio Reglamento. El Grupo de Trabajo del Artículo 29 desarrolló las llamadas reglas corporativas vinculantes o *Binding Corporate Rules* (en adelante, BCR), como alternativa a los *Safe Harbor* (vigentes en aquel momento) y a las cláusulas modelo de la Unión Europea. Son adicionales a las cláusulas contractuales tipo y pueden utilizarse para complementarlas. El Grupo de Trabajo del Artículo 29 ha redactado algunos informes[259] que completan su contenido y procedimiento previo, y que las adaptan para extender su uso para encargados del tratamiento[260]. El nuevo Reglamento General de Protección de Datos pretende fomentar y generalizar la adopción de las BCR dentro de los grupos multinacionales, flexibilizando el proceso de aprobación por las autoridades de control[261].

Sobre los instrumentos mencionados que permiten garantizar la legalidad de las transferencias internacionales de datos en los servicios de computación en nube, nos adherimos a lo manifestado por GUASCH PORTAS y SOLER FUENSANTA: "hay que ser conscientes de que la existencia de estos instrumentos para garantizar la legalidad de las transferencias internacionales en el ámbito de la computación en nube no elimina las dificultades de su implantación en muchos casos reales. Deberán surgir nuevas herramientas en el futuro para facilitar todavía más el cumplimiento de las normas sobre protección de datos, tanto por parte del cliente como por parte del proveedor de servicios"[262].

---

259 Concretamente, los siguientes informes del Grupo de Trabajo del Artículo 29: WP 155 (Preguntas más frecuentes sobre *Binding Corporate Rules*), WP 154 (Estructura de las *Binding Corporate Rules*), WP 153 (elementos y principios que deben recoger las *Binding Corporate Rules*), WP 108 (modelo de solicitud de autorización de transferencia internacional basado en *Binding Corporate Rules* dentro del procedimiento coordinado), WP 107 (competencias de las autoridades de control en el procedimiento coordinado de aprobación de las *Binding Corporate Rules*) y WP 74 (Documento sobre la aplicación del artículo 26.2 de la Directiva 95/46/CE a las *Binding Corporate Rules*).

260 En concreto, estas *Binding Corporate Rules* para encargados se exponen en los *Documentos Explicativos sobre las normas corporativas vinculantes para encargados del tratamiento*, de abril de 2013 (WP 204) y su versión revisada de mayo de 2015.

261 Considerandos 108 y 110, y art. 47 del Reglamento General de Protección de Datos.

262 GUASCH PORTAS, Vicente; SOLER FUENSANTA, Juan Ramón; "*Cloud Computing,* cláusulas contractuales y reglas corporativas vinculantes", *Revista de Derecho UNED*, núm. 14, 2014, págs 247 a 269. Compartimos asimismo la posición de GUASCH PORTAS, quien manifiesta

Para terminar con la normativa aplicable en la actualidad, debemos recordar que constituye una falta leve según el art. 44.2.d) de la LOPD la transmisión de datos a un encargado de tratamiento sin la firma de un contrato de acceso a datos, sancionada con multa de 900 a 40.000 €; y una falta muy grave, de acuerdo con lo dispuesto en el artículo 44.4.e) de la LOPD, "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", y que conlleva sanciones de 300.000 a 600.000 €, riesgo que podría llevar a muchas pequeñas y medianas y empresas a la quiebra financiera.

4.2.3.- Las transferencias internacionales de datos en el nuevo Reglamento General de Protección de Datos

El nuevo Reglamento General de Protección de Datos, que será aplicable a mediados del año 2018, establece en su artículo 44 que "solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional", y que "todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado".

Así, tras prohibir las transferencias internacionales de datos personales que no cumplan con las condiciones establecidas en la propia norma se refiere a las transferencias basadas en una decisión de la Comisión Europea (por ejemplo, el acuerdo *Shield*) en la que se considere que el destinatario (tercer país, territorio, sector u organización internacional) ofrece las garantías adecuadas para recibir y tratar datos personales de ciudadanos europeos (artículo 45 del Reglamento

---

la necesidad de una regulación específica para las transferencias internacionales de datos que ofrecen un nivel adecuado de protección, motivado por el masivo flujo de datos que tiene lugar entre entidades privadas y públicas de países diversos, a través de la tecnología. GUASCH PORTAS, Vicente, *La transferencia internacional de datos en las normativas española y comunitaria,* 1ª edición, Madrid, 2014, 336 págs. Respecto de la misma cuestión, según ALVAREZ RIGAUDIAS, las principales dificultades en las transferencias internacionales dentro de la computación en nube son las cuestiones técnicas, el coste en factor tiempo y la documentación jurídica que requiere de conocimiento especializado. Por ello la autora considera necesario la adopción de esquemas más flexibles. ALVAREZ RIGAUDIAS, Cecilia, "Condiciones para las transferencias internacionales de datos personales en servicios Cloud", *Derecho y Cloud Computing* (Coord. Ricard Martínez Martínez), Navarra, 2012, pág. 145.

europeo). A falta de esta decisión de la Comisión, el artículo 46 del Reglamento europeo afirma que es posible realizar transferencias internacionales de datos de ciudadanos europeos si los receptores de estas transferencias acreditan el cumplimiento de las garantías adecuadas mediante un instrumento jurídicamente vinculante y exigible ante las autoridades, normas corporativas vinculantes, cláusulas tipo adoptadas por la Comisión o por una autoridad de control (de acuerdo con el artículo 93.2 del Reglamento europeo), códigos de conducta o mecanismos de acreditación válidamente adoptados (art. 40 del Reglamento europeo) junto con compromisos vinculantes y exigibles del responsable o encargado del tercer país en cuanto a aplicar estas garantías y permitir el ejercicio de los derechos de los interesados. Además, los interesados deberán contar con derechos exigibles y acciones legales efectivas (art. 46.1 del Reglamento)[263].

Estas garantías que demuestren la adecuación de la transferencia pueden ser igualmente aportadas por un contrato entre responsable o encargado y el destinatario del tercer país, cuando así lo autorice la autoridad de control competente, de acuerdo con el apartado 3 del artículo 46 del Reglamento europeo[264].

Como conclusión, opinamos que, una vez que sea de aplicación en nuevo Reglamento europeo, la mayoría de transferencias internacionales que tengan lugar como consecuencia de contratos de computación en la nube entre clientes *cloud* responsables del tratamiento y proveedores *cloud* encargados del tratamiento, o

263 Artículo 46 del Reglamento General de Protección de Datos. "1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. 2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por: a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos; b) normas corporativas vinculantes de conformidad con el artículo 47; c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2; d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2; e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados. (...)".

264 Artículo 46.3 del Reglamento General de Protección de Datos. "Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante: a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados".

entre encargados y subencargados, serán legitimadas mediante decisiones de la Comisión (como el acuerdo *Shield* y la adscripción a este por parte de los proveedores *cloud* destinatarios de los datos), la suscripción de contratos que obtengan la autorización de la autoridad de control competente o que se suscriban a través de cláusulas tipo, o, en caso de transferencias de datos entre filiales de empresas multinacionales, a través de normas corporativas vinculantes. Por ello, el pequeño empresario responsable del tratamiento debe constatar la adecuación del proveedor elegido al cumplimiento legal del marco europeo a través de estos instrumentos.

4.3.- La transferencia de datos personales entre PYME españolas y proveedores norteamericanos de *Cloud Computing* tras la reciente anulación del Acuerdo *Safe Harbor* por el TJUE

De acuerdo con la Decisión 2000/520/CE, los principios *Safe Harbor* eran un compromiso de adopción voluntaria que suscribían entidades importadoras de datos personales radicadas en EE. UU.[265], y cuya adscripción solía reflejarse en el contrato de suscripción del servicio, en especial en sus políticas de privacidad[266]. Así, esta Decisión no reconocía que todo el territorio estadounidense tuviera un nivel de protección con garantías equiparables al sistema europeo, sino que las empresas norteamericanas suscriptoras de los principios de puerto seguro se comprometían a mantener ciertas garantías en cuanto al tratamiento de datos personales procedentes de empresas europeas[267].

265 La lista de entidades adherentes está disponible en la página web oficial del Departamento de Comercio de EE. UU. Disponible en: <https://safeharbor.export.gov/list.aspx>. Entre ellas encontramos proveedores *cloud*, como Amazon, Facebook, Microsoft o Apple. [Fecha de consulta: 15 de mayo de 2017].

266 A modo de ejemplo, la política de datos de *Facebook* [en línea] afirma que "Facebook. Inc. ha obtenido la certificación del marco Escudo de la privacidad Unión Europea-Estados Unidos emitida por el Departamento de Comercio de Estados Unidos en lo que concierne a la recopilación y el procesamiento de datos personales de nuestros anunciantes, clientes o socios comerciales en la Unión Europea ("Socios"), con relación a los productos y servicios descritos en la sección "Alcance" incluida más adelante y en nuestra certificación". Disponible en: <https://m.facebook.com/about/privacyshield>. [Fecha de consulta: 15 de mayo de 2017].

267 Aunque este sistema ya recibió numerosas críticas desde su aprobación, entre las que destacaban las efectuadas por el Grupo de Trabajo del Artículo 29 en su Opinión 4/2000 sobre el nivel de protección que proporcionaban los principios de puerto seguro, siguió utilizándose este sistema por motivos políticos y comerciales.

Recientemente, como es sabido, la Decisión 2000/520/CE 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" referentes a tal acuerdo, publicadas por el Departamento de Comercio de Estados Unidos en su página web), ha sido declarada nula por el TJUE, en el marco del conocido caso "Europa vs *Data Protection Comissioner*[268]". Así lo declaró la Gran Sala del Tribunal de Justicia de la Unión Europea, en fecha 6 de octubre de 2015, y resolviendo el litigio "Maximillian Schrems" contra el *Data Protection Comissioner* (Comisario para la Protección de Datos), caso C-362/2014, acerca de la negativa de este a instruir una reclamación presentada por el Sr. Schrems[269].

En fecha 2 de febrero de 2016, la Comisión Europea y los Estados Unidos acordaron un nuevo marco para permitir la transferencia transatlántica de datos: el llamado "Shield" o "Escudo de la privacidad UE- EE. UU."[270]. Este nuevo marco incorpora mecanismos más garantes respecto de la protección de datos de ciudadanos europeos que se transmitan a EE. UU[271]. En primer lugar, se les impondrá a esas

268 Maximillian Schrems forma parte del colectivo *Europa vs. Facebook,* que persigue una mayor transparencia en cuanto al tratamiento de datos personales que realiza la sede europea de *Facebook (Facebook Ireland Ltd)*, que las opciones sobre privacidad que se aplican por defecto sean más respetuosas con la privacidad del usuario, datos del usuario no necesarios para la prestación del servicio, o la falta de garantías en cuanto a la retención y borrado de datos. Información disponible en: <http://www.europe-v-facebook.org/ES/Objetivos/objetivos.html>. [Fecha de consulta: 15 de mayo de 2017]

269 Para más información sobre el Caso Schrems, nos remitimos a ROSSELLÓ RUBERT, Francisca Mª; "La transferencia de datos personales entre PYME españolas y proveedores norteamericanos de Cloud Computing tras la reciente anulación del Acuerdo Safe Harbor por el Tribunal de Justicia de la Unión Europea", *Diario La Ley*, núm. 8725, 2016.

270 Este acuerdo, adoptado finalmente el 12 de julio de 2016, se consideró plenamente operativo en fecha 1 de agosto de 2016, con la pretensión de que este nuevo marco sea el sucesor de la anulada Decisión 2000/520/CE. Supondrá que las empresas que se adhieran a este nuevo esquema garantizan un nivel de protección adecuado que asegura a los ciudadanos europeos titulares de datos personales el cumplimiento del marco europeo de privacidad, y a los responsables y encargados del tratamiento europeos la adecuación a las exigencias leales en cuanto a transferencias internacionales de datos de carácter personal. Toda la información sobre el Acuerdo *Shield* se encuentra publicada en el sitio web de la Comisión Europea. Además, la Comisión ha redactado una guía para la máxima comprensión del ciudadano de las consecuencias de la adopción de este acuerdo y de las obligaciones de las empresas norteamericanas que se han adherido a sus compromisos. Disponibles respectivamente en: <http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm> y <http://ec.europa.eu/justice/data-protection/document/citizens-guide_en.pdf>.[Fecha de consulta: 15 de mayo de 2017].

271 El texto del Acuerdo *Shield* está disponible en el sitio web de la Unión Europea. Disponible en:<http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016D1250&from=EN>.

empresas obligaciones más estrictas en cuanto al tratamiento de datos personales procedentes de la Unión Europea, se las someterá a un mayor seguimiento y ejecución al Departamento de Comercio de los Estados Unidos y a la Comisión Federal de Comercio, y pueden ser sancionadas ante incumplimientos de lo acordado. En segundo lugar, las el acceso de las autoridades públicas norteamericanas podrá limitarse y controlarse cuando afecte a datos personales transferidos bajo el amparo del "Escudo de privacidad", según ha garantizado el gobierno norteamericano. Es más, el funcionamiento de este nuevo mecanismo contra la vigilancia masiva indiscriminada de datos personales transmitidos hacia este país se llevará a cabo a través de la figura del "Defensor del Pueblo", perteneciente al Departamento de Estado.

Además, se ponen a disposición de los ciudadanos europeos diferentes vías de recurso para aquellos casos en que puedan considerar que sus datos transferidos a EE. UU. se utilicen indebidamente, tales como plazos de respuesta de las empresas (por ejemplo, proveedores *cloud* norteamericanos adscritos al programa "Shield") ante peticiones de los ciudadanos europeos, reclamaciones por parte de autoridades europeas de protección de datos al Departamento de Comercio a instancias de los interesados, o el acceso gratuito a mecanismos de solución de conflictos alternativos a la jurisdicción. La aparición de la mencionada figura del Defensor del Pueblo es otra garantía más del ciudadano europeo, figura independiente de los Servicios de Inteligencia, será el encargado de tratar cuestiones relacionadas con el acceso a información por parte de las autoridades de seguridad nacional norteamericanas[272].

[Fecha de consulta: 15 de mayo de 2017].

272 Por su parte, el Grupo de Trabajo del Art. 29 publicó el 13 de abril de 2016 su opinión sobre el borrador del acuerdo entre Estados Unidos y la Unión respecto de la decisión de adecuación "Shield". En primer lugar, celebraba la rápida adopción de un nuevo acuerdo reforzado y más garantista, solo cinco meses después de la invalidación del anterior acuerdo *Safe Harbor*. Además, agradecía las mejoras en cuanto a la transparencia. Sin embargo, recomendaba mejoras respecto de algunos aspectos: la existencia de un verdadero derecho a la oposición al tratamiento y la falta de regulación de las decisiones automatizadas, la obligación de borrar los datos remanentes en las empresas una vez que dejen de ser necesarios para el tratamiento; la no exclusión absoluta por parte de la administración norteamericana de la recolección indiscriminada de datos personales; y respecto del mecanismo del Defensor del Pueblo, si tendrá la suficiente potestad como para permitir su funcionamiento independiente, y que se aporten garantías en cuanto a esa independencia. Además, realiza otras sugerencias, como anexionar al texto un conjunto de definiciones acordadas entre Estados Unidos y la Unión Europea, con la intención de clarificar las principales nociones. En un comunicado de 12 de julio de 2016, el Grupo de Trabajo se lamenta de que algunas de estas sugerencias no hayan tomado forma en el texto definitivo. Opinión del Grupo de Trabajo del Artículo 29 sobre el Acuerdo Shield ("Opinion 01/2016 on the EU - U.S. Privacy

Todos estos mecanismos se someterán a una revisión anual por parte de la Comisión Europea y el Departamento de Comercio norteamericano, en la cual participarán también expertos de los servicios de inteligencia y autoridades europeas de protección de datos.

De todos modos, recordemos que la adscripción de las empresas norteamericanas (entre ellas, prestadores norteamericanos de servicios *cloud*) a este acuerdo es voluntaria, así que el pequeño empresario responsable del tratamiento deberá asegurarse, antes de contratar servicios *cloud* prestados por empresas norteamericanas, de que estas empresas efectivamente se han adscrito al acuerdo "Shield". El pequeño empresario deberá realizar esta comprobación hasta que entre en vigor el nuevo Reglamento europeo que, como recordaremos, ha ampliado su ámbito de aplicación territorial y vinculará a aquellas empresas que traten datos de ciudadanos europeos en el marco de la oferta de bienes y servicios o monitorizaciones de comportamiento, según su artículo 3.2.

Por último, cabe destacar que la sentencia del Tribunal de Justicia de la Unión Europea puede tener consecuencias también para otras decisiones sobre adecuación en materia de privacidad previamente tomadas por la Comisión Europea, puesto que reconoce a las autoridades nacionales la potestad de investigar si se sigue garantizando de manera efectiva, tras el transcurso del tiempo, el nivel adecuado de protección. La sentencia del Tribunal de Justicia de la Unión Europea recuerda a las autoridades de control nacionales que tienen competencia para investigar de forma independiente si una transferencia de datos a un tercer país cumple con las exigencias de la Directiva, y a suspender las transferencias de datos cuando el país receptor no garantice un nivel adecuado de protección de los datos personales, aun cuando previamente la comisión Europea se haya manifestado a través de una Decisión en la que se considere que ese país tiene un nivel de protección adecuado.

Shield draft adequacy decision",WP238) [en línea]; Comunicado del Grupo de Trabajo del artículo 29 sobre el acuerdo *Shield*, de fecha 12 de julio de 2016 ("Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield") [en línea] y FAQs sobre Shield que responden a la preguntas más frecuentes sobre el Acuerdo *Shield*, a modo de guías (una dirigido a empresas europeas y otra a titulares de datos personales), disponibles respectivamente en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf>, <http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf> y <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083>. [Fecha de consulta: 15 de mayo de 2017].

5.- LA IMPORTANCIA DEL CONTRATO ENTRE PROVEEDOR Y CLIENTE. LAS POLÍTICAS DE PRIVACIDAD

Es preciso que el suscriptor de servicios de computación en la nube revise las condiciones contractuales puestas a disposición por el proveedor, para asegurarse la adecuada previsión sobre las finalidades del tratamiento, las transferencias de datos personales y el destino de la información una vez terminada la relación contractual, tanto si es un titular de datos personales quien contrata, como si es un pequeño empresario que utilizará esos servicios como herramienta para tratar datos de carácter personal de terceros y, como tal, asumirá el papel de responsable del tratamiento.

Tal y como sucede en la mayoría de documentos legales incorporados o anexos a los contratos en línea y en sitios de Internet en los que el usuario crea una cuenta, en la práctica contractual de suscripción de servicios de computación en la nube a menudo encontramos apartados expresamente dedicados a las políticas de privacidad del proveedor. Estas políticas suelen contener:

a) El tipo de información que se requiere para proporcionar los servicios: datos de identificación y facturación del usuario, datos de los contactos que tiene usuario, fotos u otros contenidos migrados, mensajes de correo electrónico, direcciones IP, información sobre dispositivos desde los cuales se realiza el acceso al servicio *cloud*, ubicación física, etc.;

b) el modo en el cual se recaban (datos introducidos por el usuario, registros automáticos del servidor, uso de *cookies* o tecnologías similares, etiquetados, monitorizaciones del uso del servicio, etc.), tratan (almacenamiento, procesamiento, tiempo de conservación de la información, realización de copias de seguridad, etc.) y eliminan los datos de carácter personal (borrado a través de sobreescritura, etc.), así como los lugares donde tiene lugar este tratamiento (Estados Unidos, Unión Europea, ubicaciones dispersas globalmente, etc.);

c) con quien se comparte o puede compartirse la información obtenida (subproveedores, socios comerciales, filiales, nuevos adquirentes en casos de fusiones o venta de activos, otros usuarios del servicio, autoridades competentes, etc.);

d) principios a los cuales se somete el tratamiento (transparencia, confidencialidad, protección de derechos de terceros, etc.) y marcos de regulación de

la política de privacidad ("Shield", Directiva 95/46/CE, certificaciones de privacidad, etc.);

e) información general sobre seguridad (uso de herramientas de encriptado o autenticación, funciones de navegación segura, etc.), adopción de estándares técnicos, y protocolos de actuación y buenas prácticas ante la detección de vulnerabilidades (alertas, publicaciones o avisos en el sitio web del proveedor, etc,)[273];

f) se obtienen las autorizaciones del responsable del tratamiento, o directamente del titular si este es consumidor, para determinados usos y finalidades del tratamiento, también detallados, y se presentan mecanismos para modificar las preferencias de privacidad, acceder a los datos, actualizarlos, modificarlos, controlar con quien se comparten, y, en su caso, ejercer los derechos otorgados legalmente[274];

---

273 En la práctica, la mayoría de proveedores ofrece información sobre las medidas de seguridad implementadas, más o menos detalladas, como el cifrado de datos en tránsito tipo *Transport Security Layer*. Por ejemplo, Google informa en su política de privacidad que "Encriptamos muchos de nuestros servicios mediante el protocolo SSL. Ofrecemos la posibilidad de configurar la verificación en dos pasos para acceder a las cuentas de Google, así como una función de navegación segura en "Google Chrome". Revisamos nuestra política en materia de recogida, almacenamiento y tratamiento de datos, incluyendo las medidas de seguridad físicas, para impedir el acceso no autorizado a nuestros sistemas. Limitamos el acceso de los contratistas, los agentes y los empleados de Google a la información personal que deben procesar para Google y nos aseguramos de que cumplan las estrictas obligaciones de confidencialidad contractuales y de que estén sujetos a las condiciones disciplinarias pertinentes o al despido si no cumplen dichas obligaciones". [En línea]. Disponible en: <http://www.google.es/intl/es/policies/privacy/> [Fecha de consulta: 15 de mayo de 2017]. Dropbox también detalla parte de las medidas adoptadas para proteger los datos: "Los archivos de Dropbox almacenados se cifran mediante el estándar Advanced Encryption Standard (AES) de 256 bits. Para proteger los datos en tránsito entre las aplicaciones de Dropbox y nuestros servidores, Dropbox emplea las tecnologías Secure Sockets Layer (SSL)/Transport Layer Security (TLS), que crean un túnel seguro protegido por un cifrado con Advanced Encryption Standard (AES) de 128 bits o superior. Comprobamos constantemente las aplicaciones y la infraestructura de Dropbox en busca de vulnerabilidades de seguridad y las reforzamos para mejorar la seguridad y protegerlas contra posibles ataques. La verificación en dos pasos ofrece una capa adicional de seguridad al iniciar sesión. Puedes elegir si prefieres recibir códigos de seguridad mediante mensajes de texto o mediante aplicaciones de contraseñas de un solo uso (TOTP) como las de esta lista. Los archivos públicos solo están disponibles para las personas que tengan un enlace a ellos". [En línea]. Disponible en: <https://www.dropbox.com/es_ES/help/27> [Fecha de consulta: 6 de septiembre de 2016]. El usuario de servicios raramente podrá incidir en el despliegue de las medidas de seguridad implementadas por defecto por parte del proveedor pero tampoco es plausible una detallada explicación de las estrategias de seguridad a los usuarios, porque pueden exponer vulnerabilidades de los sistemas. Sería adecuado reflejar contractualmente que, si producen incidencias de seguridad que afecten a los datos personales de los que es responsable el cliente del servicio de *Cloud Computing*, se le comuniquen al responsable, junto con las medidas adoptadas para mitigar los daños producidos. Las políticas de privacidad suelen ser proteccionistas en cuanto a la distribución de responsabilidades entre cliente y proveedor, eximiéndose en ocasiones de cualquier responsabilidad por brechas de seguridad que afectan a datos personales.

274 Así lo recogen Dropbox o Google en sus políticas de privacidad [en línea]. Disponibles

Puesto que el problema principal radica en la imposibilidad de negociar los contratos de adhesión, y, consecuentemente, la legislación aplicable en materia de privacidad, el pequeño empresario suscriptor de estos servicios deberá asegurarse, antes de contratar, de que el proveedor ofrece las suficientes garantías, dado que a él le corresponde la responsabilidad por la elección de un encargado del tratamiento que le permita asegurar el cumplimiento de la normativa europea y española en materia de protección de datos. Si la normativa aplicable en materia de privacidad es la LOPD, las relaciones entre responsable y encargado deberán recogerse de manera detallada en el contrato exigido por los artículos 12 de la LOPD y 21 del RLOPD. Por tanto, corresponderá al responsable averiguar si este contrato entre responsable y encargado ofrecido por el proveedor a modo de contrato de adhesión cumple los requisitos exigidos por la LOPD y el RLOPD. En muchas ocasiones, como se ha dicho, el proveedor *cloud* agrupa este conjunto de cláusulas contractuales referentes a la privacidad en una parte del acuerdo contractual que suele denominarse "política de privacidad". En caso de que tal acuerdo sobre privacidad no cumpla con los requisitos de contenido contractual exigidos por los artículos de la LOPD y del RLOPD mencionados, el empresario responsable del tratamiento deberá proponer los cambios necesarios al proveedor *cloud*, o sustituir sus servicios por los de otro proveedor, para asegurarse en todo caso el cumplimiento legal.

En cuanto a las reclamaciones que pretenda interponer el cliente *cloud* pequeño empresario por incumplimiento de las políticas de privacidad, será necesario acudir al contrato suscrito y a la modalidad de servicio de nube pública contratado[275], comprobar las responsabilidades asumidas por responsable, encargado y, en su caso, subencargado, y, atendiendo a la legislación aplicable a la política de privacidad, analizar las consecuencias derivadas del eventual incumplimiento, los mecanismos de prueba con los que cuenta el pequeño empresario, las posibles acciones que pueda interponer contra el proveedor incumplidor en base al incumplimiento contractual, y qué autoridades son competentes para conocer del caso.

El interesado, por su parte, puede reclamar directamente ante la Agencia Española de Protección de Datos por el incumplimiento de la normativa actual (art.

---

respectivamente en: <https://www.dropbox.com/es_ES/privacy> y <http://www.google.es/intl/es/policies/privacy/>. [Fecha de consulta: 15 de mayo de 2017].

275 Ver Figura 2, en el apartado "Modelos de servicio de computación en la nube" del capítulo "Concepto y características técnicas de la computación en la nube".

18 LOPD[276]), en cuyo caso se iniciará el pertinente procedimiento administrativo sancionador; y ante el responsable o el encargado del tratamiento que les haya podido ocasionar daños en sus bienes o derechos, para que estos sean reparados (como se verá a continuación, art. 19 LOPD).

Por último, cabe destacar los beneficios de una buena redacción de la política de privacidad: mejor protección a los interesados y a los clientes *cloud* profesionales; más claridad en la distribución de responsabilidades entre proveedor *cloud* y cliente pequeño empresario; mayor seguridad jurídica y transparencia en cuanto al tratamiento de datos personales; y mejor cumplimiento del pequeño empresario (en su papel de responsable del tratamiento) con las instrucciones del interesado, con eventuales requerimientos de las autoridades, y con las exigencias de la normativa aplicable en materia de protección de datos.

6.- RESPONSABILIDAD POR INCUMPLIMIENTO DE OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS

En cuanto a la responsabilidad por incumplimiento de obligaciones en materia de protección de datos, es la obligación del responsable elegir un encargado o encargados que proporcionen las suficientes garantías (art. 17.2 Directiva 95/46/CE, art. 20.2 RLOPD y art. 28.1 del Reglamento General de Protección de Datos)[277].

El titular de los datos podrá reclamar por los daños derivados de la intromisión ilegítima en su privacidad debido al incumplimiento de la LOPD. Así se desprende del artículo 19.1 de la LOPD: "Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados". Por ello, si, este incumplimiento tiene lugar en el marco de una prestación de servicios de computación en la nube, el interesado perjudicado podrá reclamar al encargado o subencargado aun cuando el daño se haya producido sin que medie una relación

276 Artículo 18 LOPD. "Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine".

277 Art. 20.2 RLOPD. "Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento".

contractual entre este interesado y el encargado o subencargado del tratamiento que lo haya provocado, ya que el nexo entre ambos nace de la intermediación del responsable del tratamiento. Por otra parte, el derecho del titular de datos personales perjudicado a ser indemnizado no impide el ejercicio de cualesquiera otros derechos que corresponden al interesado en virtud de la normativa en materia de protección de datos (derecho al acceso, rectificación, cancelación, etc.).

Como puede observarse, la posibilidad de reclamación que prevé el artículo 19.1 de la LOPD se refiere únicamente al interesado perjudicado, pero no determina cómo puede protegerse al potencial responsable del tratamiento que haya tenido que indemnizar al perjudicado por el incumplimiento de la normativa de protección de datos por parte de un subencargado del tratamiento, más aun si el contrato suscrito con el encargado exime de responsabilidad al proveedor principal por actuaciones del subcontratista infractor en materia de protección de datos[278].

El grupo de expertos en contratación de la *Cloud Computing Strategy* plantea la posibilidad, por una parte, de habilitar acciones directas del empresario responsable del tratamiento contra el subproveedor *cloud* y, por otra, de que el proveedor *cloud* tuviera que responder por toda la cadena de subcontrataciones ante el cliente[279]. Por nuestra parte, nos decantamos por un proveedor *cloud* que responda por toda la cadena de subcontrataciones ante el suscriptor (independientemente de que posteriormente pueda repetir contra los subcontratistas infractores) por ser la solución más transparente y sencilla para pequeños empresarios, si bien también consideramos que sería adecuado un sistema de responsabilidad solidaria complementario, en el cual el responsable del tratamiento pudiera interponer su acción tanto ante el encargado como ante el subencargado. Como veremos más adelante, el Reglamento General de Protección de Datos ha establecido que sea el encargado del tratamiento quien responda por los incumplimientos en materia de protección de datos de sus subcontratistas ante el responsable del tratamiento.

Por su parte, el Grupo de Trabajo del Artículo 29 pone como ejemplo, en el mencionado Dictamen 5/2012 sobre *Cloud Computing*, las cláusulas contractuales

278 Ver apartado "La responsabilidad del proveedor por actuaciones de los subproveedores", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

279 CLOUD COMPUTING STRATEGY, *Discussion Paper on Subcontracting*, pág. 3, [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/files/expert_groups/expert_group_subcontracting_discussion_paper_en.pdf>. [Fecha de consulta: 6 de septiembre de 2016].

tipo para la transferencia internacional de datos personales a encargados del tratamiento establecidos en terceros países, introducidas por la Decisión de la Comisión de 5 de febrero de 2010. Mediante estas cláusulas, el subtratamiento se permite únicamente si se cumplen dos requisitos: el primero, que exista autorización previa y por escrito del responsable; el segundo, que medie un acuerdo escrito a través del cual el encargado responda plenamente frente al responsable por la ejecución de las obligaciones del subencargado. El Grupo de Trabajo del Artículo 29 recomienda introducir cláusulas de contenido similar en los contratos de computación en la nube entre el empresario suscriptor (responsable del tratamiento) y aquel proveedor *cloud* principal (encargado del tratamiento) que prevea prestar o que preste los servicios mediante subcontratación, para garantizar así que la cadena de subcontrataciones no dispersa las obligaciones y responsabilidades en materia de protección de datos. Esta sería, a nuestro parecer, una buena solución ante posibles reclamaciones del responsable del tratamiento, aunque en la práctica contractual será el propio proveedor *cloud* quien decida incluir o no estas cláusulas de asunción de responsabilidad por incumplimientos en materia de protección de datos por parte de subproveedores en el contrato predispuesto, a modo de buena práctica. Recordemos que, de manera general, el pequeño empresario suscribe el contrato *online* que le ofrece el proveedor *cloud* y carece de posibilidad de negociación.

Una vez que resulte aplicable, el Reglamento General de Protección de Datos establece, al igual que lo hace la actual LOPD, que "Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos" (art. 82.1). Pero además, el Reglamento determina que quien debe indemnizar al interesado perjudicado es el responsable del tratamiento, que responderá por todos los daños y perjuicios ocasionados por el tratamiento, y que el encargado únicamente debe responder cuando haya incumplido las instrucciones del responsable o las obligaciones que el Reglamento impone directamente al encargado (art. 82.2[280]). Recordemos que será responsabilidad del pequeño empresario elegir un proveedor *cloud* que ofrezca las garantías suficientes como para garantizar el cumplimiento del Reglamento europeo y la protección de la privacidad del titular de los datos

280 Artículo 82.2 del Reglamento General de Protección de Datos. "2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable".

personales (art. 28.1 del Reglamento europeo). Posteriormente, el responsable del tratamiento que haya abonado la indemnización podrá interponer un recurso contra otros responsables o encargados que hayan participado en el tratamiento (art. 82.5 del Reglamento europeo[281]). Los encargados del tratamiento que hayan subcontratado tales operaciones del tratamiento, en virtud del artículo 28.4 del Reglamento, responderán por los incumplimientos de los subencargados en materia de protección de datos: "Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado".

La aplicación del nuevo Reglamento europeo supondrá que el pequeño empresario suscriptor de servicios *cloud* responsable del tratamiento deberá ser quien indemnice, en primer lugar, al interesado perjudicado. Posteriormente, el pequeño empresario podrá, en su caso, repetir contra el proveedor *cloud* encargado del tratamiento, y este estará obligado legalmente a responder por aquellos sucontratistas que hayan incumplido sus obligaciones en materia de protección de datos.

Una vez extinguido el contrato entre proveedor *cloud* y subproveedor, el proveedor *cloud* principal debe asegurarse de que la transición hacia un nuevo subproveedor se produce con éxito y que se dará cumplimiento a todas las obligaciones que mantiene con el cliente pequeño empresario. Así, por una parte, deberá asegurar que se cumple con aquellas obligaciones derivadas de la normativa de protección de datos respecto de la extinción del contrato con el antiguo subproveedor (recuperación de datos por parte del cliente, destrucción de copias, borrado, etc.), como indica el art. 12.3 LOPD[282]), y, por otra parte, garantizar que se sigue cumpliendo con lo acordado en la relación contractual con el cliente que todavía sigue vigente (disponibilidad del servicio, calidad de los recursos suministrados, resto de obligaciones en materia de protección de datos, etc.).

281 Artículo 82.5 del Reglamento General de Protección de Datos. "Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2".

282 Art. 12.3 LOPD: "Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

7.- LOS EFECTOS DE LA FINALIZACIÓN DEL CONTRATO DE COMPUTACIÓN EN LA NUBE SOBRE LOS DATOS PERSONALES

Una vez finalizada la prestación contractual que habilita al encargado al acceso a los datos de carácter personal, el art. 12.3 LOPD exige el retorno de los datos a su responsable o la destrucción del soporte que los contiene[283]. De igual manera, el artículo 22.1 del RLOPD contempla la devolución de los datos o del soporte que los contiene no como un derecho del interesado, sino como una alternativa al borrado en cuanto a destino de los datos una vez se haya extinguido la relación contractual entre titular de datos personales y responsable o entre responsable y encargado del tratamiento[284]. El artículo no determina si es el responsable del tratamiento quien debe decidir sobre la devolución o borrado de los datos o si se realizará a elección del encargado del tratamiento que los debe devolver o borrar.

Con la normativa aplicable actualmente, será recomendable que el responsable, antes de elegir el proveedor *cloud*, se informe sobre las soluciones específicas que ofrece en cuanto a portabilidad, atendiendo al tipo de servicio y a la modalidad de nube implementada, especialmente cuando se hayan migrado datos de carácter personal[285]. Cabe decir que, en el marco del contrato de servicios de computación en la nube pública que impliquen las migraciones de datos del suscriptor (sean o no de carácter personal), la puesta a disposición del cliente de los datos migrados durante el uso del servicio *cloud* para que este pueda instalarlos en su propio sistema informático o transmitirlos a otro proveedor forma parte de las obligaciones del proveedor que se derivan de la propia naturaleza del contrato de servicios de computación en la nube, así como facilitar al cliente información sobre el formato de recuperación de estos datos[286].

---

283 Art. 12.3 LOPD. "Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

284 Art. 22.1 RLOPD. "Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. (...)".

285 Para un análisis más detallado, nos remitimos a ROSSELLÓ RUBERT, Francisca Mª, "La recuperación de los contenidos alojados y su portabilidad; en especial, su previsión por el Reglamento 2016/679 General de Protección de Datos de la UE", *Hacia una justicia 2.0, Actas del XX Congreso Iberoamericano de Derecho e Informática* (Dir. Federico Bueno de Mata), Salamanca, 2016, págs. 283 a 298.

286 Ver apartado "La recuperación de los datos alojados en la nube por el cliente y su portabilidad a otro proveedor", en el capítulo "Modificación, suspensión y extinción del contrato

Así, por una parte, hablaremos de recuperación de datos cuando se le devuelvan al cliente los datos y soportes que los almacenan y, por otra, de portabilidad, en cuanto a la posibilidad de transferirlos de manera sencilla de un sistema a otro sin necesidad de volver a introducirlos, tal y como se ha visto en apartados anteriores[287]. Según la Agencia Española de Protección de Datos, los servicios de computación en la nube serán abiertos a la portabilidad cuanto mayor sea la facilidad de un usuario para transferir todos sus datos y aplicaciones desde un proveedor a otro, o a los sistemas propiedad del cliente, garantizando la disponibilidad de los datos y la continuidad del servicio. Cuanto más cerrado a la portabilidad sea el servicio, será más difícil, o incluso no factible, el retorno de los datos a un coste razonable, y puede que ello obligue al cliente a permanecer con ese proveedor si no quiere renunciar a los contenidos migrados[288].

La Agencia Española de Protección de Datos considera que el proveedor debe obligarse, una vez terminado el contrato, a entregar toda la información al cliente en un formato que le permita almacenarlo en sus propios sistemas y/o que permita su traslado al entorno de otro proveedor u proveedores, con total garantía de la integridad de la información y sin costes adicionales. Es recomendable que estos formatos se basen en estándares abiertos o en los estándares de portabilidad que se adopten generalizadamente por el sector[289].

---

de servicios de computación en la nube".

287 Para más detalle sobre la recuperación y la portabilidad de cualesquiera datos migrados en servicios de computación en la nube, nos remitimos al apartado "La recuperación de los contenidos alojados en la nube por el cliente y su portabilidad a otro proveedor *cloud*", en el capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

288 AEPD, *Guía para clientes que contraten servicios de Cloud Computing* [en línea]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf>. [Fecha de consulta: 6 de septiembre de 2016].

289 Existen diversas instituciones que trabajan en la adopción de estándares de interoperabilidad, portabilidad y seguridad. Una de ellas es la *Cloud Standards Coordination* (CSC) que trabaja en el marco de la ya mencionada *Cloud Computing Strategy* de la Comisión Europea y que ha publicado una lista de estándares y especificaciones relevantes para la computación en la nube y de adopción voluntaria para los proveedores, con la finalidad de su simplificación, unificación y normalización. Sitio web disponible en: <http://csc.etsi.org/phase%201/StandardsAndSpecs.html>. [Fecha de consulta: 6 de setpiembre de 2016]. En noviembre de 2013, la CSC publicó su informe final en relación al cumplimiento de la tarea encomendada por la comunicación de la Comisión "*Unleashing the Potential of Cloud Computing in Europe* (Bruselas, COM (2012) 529 final), y más concretamente la "Acción 1: acabar con la jungla de estándares" [en línea]. Disponible en: <http://csc.etsi.org/resources/CSC-Deliverable-008-Final_Report-V1_0.pdf>. [Fecha de consulta: 6 de septiembre de 2016].

Debe tenerse en cuenta, además, que la terminación del contrato puede tener lugar por causas ajenas al cliente, como por ejemplo la imposibilidad del proveedor de continuar con su operativa (como el caso de que se extinga la empresa proveedora o cesen sus actividades empresariales) o cambios en su política comercial o del marco regulatorio[290]. Asimismo, el proveedor debe permitir la recuperación de los datos personales cuando el cliente responsable del tratamiento considere inadecuada la intervención de algún subcontratista o la transferencia de datos a países que no aporten suficientes garantías, o cuando se produzcan modificaciones unilaterales de las condiciones del servicio.

Por su parte, el Grupo de Trabajo del Artículo 29, en su Dictamen 5/2012 sobre *Cloud Computing* aconseja al cliente *cloud* que compruebe las condiciones de portabilidad de los datos entre diferentes proveedores de servicios en la nube, así como su adecuación a estándares entre formatos e interfaces que permitan la interoperabilidad, para evitar que la terminación de servicios con un proveedor implique la imposibilidad de recuperar sus datos o transferirlos a otros proveedores con quienes posteriormente se suscriban los servicios.

El nuevo Reglamento General de Protección de Datos reconoce expresamente el derecho a la portabilidad, en su artículo 20. En cuanto a su estudio más detallado, nos remitimos a lo explicado al respecto en este mismo capítulo[291]. En cuanto a la portabilidad de los datos migrados a sistemas del proveedor que no tengan carácter personal, nos remitimos al apartado dedicado a tal cuestión en posteriores capítulos[292].

En ocasiones, y cuando sea de aplicación alguna disposición legal que así lo imponga, el encargado del tratamiento deberá conservar los datos, de acuerdo con el artículo 22.2 del RLOPD[293]. Durante el periodo de conservación, los datos deben estar bloqueados, es decir, no pueden someterse a ningún tratamiento que exceda de la propia conservación y del mantenimiento de las medidas de seguridad que

290 Ver capítulo "Modificación, suspensión y extinción del contrato de computación en la nube".

291 Ver apartado "Los nuevos derechos reconocidos en el Reglamento General de Protección de Datos. Especial referencia al derecho a la portabilidad y a su aplicación en los servicios de computación en la nube", en este mismo capítulo.

292 Ver apartados "La recuperación de los contenidos alojados por el cliente y su portabilidad a otro proveedor *cloud*", en el capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

293 Art. 22.2 RLOPD. Conservación de los datos por el encargado del tratamiento. "El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento".

garanticen su integridad y confidencialidad. En caso contrario, y como regla general, los datos deberán destruirse o ser devueltos al responsable.

Para que la imposibilidad de acceso a los datos sea efectiva, deberán destruirse tanto los ficheros que obren en *hardware* del encargado como todos aquellos datos transferidos y localizados en instalaciones de terceros, independientemente de su ubicación[294].

En términos informáticos, debe considerarse el concepto de borrado seguro como alternativo a la destrucción de los datos, porque la destrucción del archivo implica la inhabilitación del dispositivo *hardware* que lo almacena (discos duros, servidores, etc.), tal y como se verá en otros capítulos[295]. De ahí que las autoridades en materia de protección de datos consideren necesaria la adopción de mecanismos que garanticen el borrado seguro de los datos siempre que lo solicite el cliente y, en todo caso, al finalizar el contrato, como por ejemplo certificaciones emitidas por el propio proveedor *cloud* o por terceros independientes[296].

294 FERNÁNDEZ ALLER; Cecilia, "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube (cloud computing)", *Revista de Derecho UNED,* núm. 10, 2012, págs. 125 a 145.

295 Para más detalles en cuanto al borrado de los datos, nos remitimos a lo mencionado al respecto de los derechos del interesado de supresión y cancelación de datos de carácter personal, en este mismo capítulo. En cuanto a las técnicas de borrado, al apartado dedicado a tal efecto respecto de cualesquiera datos almacenados en la nube, y no solo para los datos de carácter personal, en los capítulos "Concepto y características técnicas de la computación en la nube" y "Modificación, suspensión y extinción del contrato de servicios de computación en la nube", especialmente el apartado "El borrado de datos como obligación del proveedor", en este último.

296 AEPD, *Guía para clientes que contraten servicios de Cloud Computing,* [en línea], pág. 18.Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf>. [Fecha de consulta: 14 de septiembre de 2016].