



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 II 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 II de II

Francisca María Rosselló Rubert

Directora: Apol·lònia Martínez Nadal

Tutora: Apol·lònia Martínez Nadal

Doctora por la Universitat de les Illes Balears

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

| | |
|---|----|
| INTRODUCCIÓN | 15 |
| CAPÍTULO PRIMERO. CONCEPTO Y CARACTERÍSTICAS TÉCNICAS DE LA COMPUTACIÓN EN LA NUBE | 24 |
| 1.- INTRODUCCIÓN | 24 |
| 2.- ¿QUÉ ES LA COMPUTACIÓN EN LA NUBE? | 26 |
| 2.1.- Definición y características técnicas según el <i>National Institute of Standards and Technology</i> (NIST) | 27 |
| 2.1.1.-1 Autoservicio bajo demanda | 28 |
| 2.1.2.- Acceso a través de la Red | 29 |
| 2.1.3.- Agrupación de recursos y <i>multi-tenancy</i> | 30 |
| 2.1.4.- Rápida elasticidad | 32 |
| 2.1.5.- Sujeción a métrica y monitorizaciones | 33 |
| 2.2.- Otras definiciones técnicas | 34 |
| 2.2.1.- Definición por el <i>American National Standards Institute</i> (ANSI)..... | 34 |
| 2.2.2.- Definición por la <i>Cloud Security Alliance</i> (CSA) | 36 |
| 2.3.- Qué no es <i>Cloud Computing</i> | 37 |
| 2.3.1.- <i>Grid Computing</i> o computación en malla | 37 |
| 2.3.2.- <i>Utility Computing</i> | 39 |
| 2.3.3.- Virtualización | 39 |
| 2.3.4.- <i>Outsourcing</i> | 40 |
| 2.3.5.- <i>Hosting</i> o alojamiento web | 42 |
| 2.3.6.- Web 2.0 | 43 |
| 3.- LA ARQUITECTURA EN CAPAS DE LA COMPUTACIÓN EN LA NUBE Y SUS PRINCIPALES MODELOS DE NEGOCIO | 47 |

ÍNDICE

| | |
|--|----|
| 3.1.- Las capas que integran la nube y su tecnología subyacente | 48 |
| 3.1.1.- La capa de hardware | 48 |
| 3.1.2.- La capa de infraestructura | 49 |
| 3.1.3.- La capa de plataforma | 49 |
| 3.1.4.- La capa de software | 50 |
| 3.2.- Los modelos de servicio en la nube | 51 |
| 3.2.1.- La infraestructura como servicio o IaaS | 52 |
| 3.2.2.- La plataforma como servicio o PaaS | 53 |
| 3.2.3.- El software como servicio o SaaS | 54 |
| 3.2.4.- Otros modelos de servicio | 58 |
| 4.- LOS MODELOS DE IMPLEMENTACIÓN DE LA NUBE | 58 |
| 4.1.- Nube privada | 59 |
| 4.2.- Nube comunitaria | 61 |
| 4.3.- Nube pública | 62 |
| 4.4.- Nube híbrida | 64 |
| 5.-DEFINICIONES JURÍDICAS DE LA COMPUTACIÓN EN LA NUBE | 66 |
| 6.- ALGUNAS CONSIDERACIONES SOBRE LA COMPUTACIÓN EN LA NUBE. EN PARTICULAR, PRINCIPALES VENTAJAS Y RIESGOS | 70 |
| 6.1.-Implementación de la computación en la nube por el sector empresarial en la actualidad. Ventajas | 71 |
| 6.2.- Riesgos de la implementación del <i>Cloud Computing</i> por parte de las empresas..... | 75 |
| 6.2.1.- Riesgos organizativos | 78 |
| 6.2.2.- Riesgos técnicos | 78 |
| 6.2.3.- Riesgos legales y retos jurídicos | 82 |

CAPÍTULO SEGUNDO. OBJETO, NATURALEZA JURÍDICA Y CARACTERÍSTICAS DEL CONTRATO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

87

| | |
|--|----|
| 1.- INTRODUCCIÓN | 87 |
| 2.- OBJETO DE LOS CONTRATOS DE COMPUTACIÓN EN LA NUBE | 89 |
| 3.- FIGURAS AFINES AL CONTRATO DE COMPUTACIÓN EN LA NUBE | 93 |

ÍNDICE

| | |
|---|----------------|
| 3.1.- El contrato de <i>Outsourcing</i> informático | 93 |
| 3.2.- El contrato de <i>Hosting</i> y de alojamiento de datos por cuenta de terceros | 97 |
| 3.3.- El contrato de suministro | 100 |
| 3.4.- El contrato de depósito | 105 |
| 3.5.- El contrato de licencia de uso no personalizada de software | 109 |
| 4.- NATURALEZA JURÍDICA DE LOS CONTRATOS DE SERVICIOS DE COMPUTACIÓN EN LA NUBE | 112 |
| 4.1.- Características de los contratos de servicios de computación en la nube..... | 112 |
| 4.1.1.- Contrato mercantil | 112 |
| 4.1.2.- Contrato consensual | 113 |
| 4.1.3.- Contrato bilateral | 115 |
| 4.1.4.- Contrato oneroso | 115 |
| 4.1.5.- Contrato de tracto sucesivo que se presta por medios electrónicos | 118 |
| 4.2.- Naturaleza jurídica del contrato de servicios de computación en la nube..... | 120 |
| 4.2.1.- El contrato de computación en la nube como contrato de arrendamiento de servicios..... | 120 |
| a) La relevancia de la contraprestación del servicio en la determinación de la naturaleza jurídica de los contratos de computación en la nube | 123 |
| b) La relevancia de las diferentes modalidades de implementación en la determinación de la naturaleza jurídica de los contratos de computación en la nube | 124 |
| 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..... | 126 |
| 4.2.2.- El contrato de computación en la nube como contrato atípico | 128 |
| 4.2.3.- El contrato de computación en la nube como contrato complejo | 130 |
| 4.3.- Definición jurídica del contrato de computación en la nube de implementación pública | 130 |
| CAPÍTULO TERCERO. ELEMENTOS SUBJETIVOS DEL CONTRATO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE | 132 |
| 1.- INTRODUCCIÓN | 132 |
| 2.- EL PROVEEDOR DE SERVICIOS DE COMPUTACIÓN EN LA NUBE | 135 |

ÍNDICE

| | |
|---|------------|
| 2.1.- El proveedor de servicios en la nube como prestador de servicios de la sociedad de la información | 137 |
| 2.2.- El establecimiento del proveedor de servicios en la nube | 141 |
| 3.- EL SUScriptor DE SERVICIOS DE COMPUTACIÓN EN LA NUBE | 144 |
| 3.1.- El empresario como destinatario. Breve referencia a sus empleados | 144 |
| 3.1.1.- El empresario como destinatario y eventualmente, subproveedor de servicios de computación en la nube | 145 |
| 3.1.2.- El rol del CTO como responsable técnico de la empresa | 148 |
| 3.1.3.- Los empleados y clientes del empresario suscriptor | 150 |
| 3.2.- El consumidor de servicios de computación en la nube | 153 |
| 3.2.1.-El concepto legal de consumidor y la eventual dificultad de su aplicación práctica en algunos contratos <i>cloud</i> | 154 |
| 3.2.2.- La protección del consumidor y su incidencia en la contratación de servicios de computación en la nube | 157 |
| 3.3.- Las Administraciones Públicas | 165 |
| 4.- TERCEROS RELACIONADOS CON EL CONTRATO DE COMPUTACIÓN EN LA NUBE | 169 |
| 4.1.- La figura del integrador de sistemas | 169 |
| 4.2.- Las entidades aseguradoras y los entornos <i>cloud</i> | 171 |
| CAPÍTULO CUARTO. ASPECTOS JURÍDICOS DE LOS CONTENIDOS ALOJADOS EN LA NUBE | 173 |
| 1.- INTRODUCCIÓN | 173 |
| 2.- CLASIFICACIÓN DE LOS DATOS ALOJADOS EN LA NUBE | 177 |
| 3.- LEGALIDAD Y ADECUACIÓN DE LOS CONTENIDOS ALOJADOS POR EL USUARIO. LAS POLÍTICAS DE USO ADECUADO (PUA) Y SU CONTROL POR EL PRESTADOR DE SERVICIOS | 180 |
| 3.1.- Las PUA en los contratos de computación en la nube | 181 |
| 3.2.- La LSSI y la responsabilidad de los prestadores de servicios en la nube por contenidos alojados | 188 |
| 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 <i>CLOUD</i> | 194 |

ÍNDICE

| | |
|--|-----|
| 4.1.- Generalidades sobre la propiedad intelectual e industrial | 195 |
| 4.1.1.- Obras protegidas por el derecho de autor | 197 |
| 4.1.2.- La protección de secretos de empresa | 198 |
| 4.1.3.- La propiedad industrial | 202 |
| 4.1.4.- Las licencias de uso | 203 |
| 4.2.- Contenidos generados fuera de la nube y migrados por el usuario | 204 |
| 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 | 205 |
| 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 | 211 |
| 4.3.- Contenidos generados por el usuario dentro del sistema <i>cloud</i> | 220 |
| 4.3.1.- Creaciones desarrolladas dentro de una relación laboral | 220 |
| 4.3.2.- Creaciones desarrolladas fuera de una relación laboral | 222 |
| 4.4.- Obras de autoría plural en la <i>nube</i> | 226 |
| 4.5.- Herramientas que el proveedor pone a disposición del cliente | 229 |
| 4.6.- Datos generados por el proveedor o por terceros a partir de la información de los usuarios | 231 |

CAPÍTULO QUINTO. PRIVACIDAD EN LA NUBE: PRINCIPALES CUESTIONES SOBRE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

237

| | |
|--|-----|
| 1.- INTRODUCCIÓN | 237 |
| 2.- MARCO NORMATIVO EUROPEO Y ESPAÑOL DE LA PROTECCIÓN DE DATOS PERSONALES | 241 |
| 3.- PRINCIPALES CONCEPTOS DE LA PROTECCIÓN DE DATOS PERSONALES Y SU TRASLADO AL ÁMBITO DE LA COMPUTACIÓN EN LA NUBE | 250 |
| 3.1.- Datos personales | 250 |
| 3.2.- Tratamiento de datos y ficheros | 253 |
| 3.3.- La asignación de los roles de titular de los datos, responsable y encargado del tratamiento en la computación en la nube | 255 |
| 3.3.1.- El titular de los datos y la prestación de consentimiento informado e inequívoco | 256 |
| 3.3.2.- El responsable del tratamiento | 264 |
| 3.3.3.- El encargado del tratamiento | 270 |

ÍNDICE

| | |
|--|-----|
| 3.3.4.- El subencargado del tratamiento | 276 |
| 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 | 285 |
| 3.4.-Medidas de seguridad según la normativa de protección de datos | 289 |
| 3.4.1.- Las medidas de seguridad exigidas por la LOPD | 289 |
| 3.4.2.- El responsable de seguridad y el documento de seguridad | 293 |
| 3.4.3.- Las medidas de seguridad en el nuevo Reglamento Europeo..... | 297 |
| 3.5.- El papel de las autoridades y de terceros independientes en materia de protección de datos | 300 |
| 3.6.-Los derechos del interesado | 304 |
| 3.6.1.- Los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) | 305 |
| 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 | 311 |
| 4.- LOCALIZACIÓN Y SEGURIDAD DE LOS DATOS. ACCESO A DATOS POR TERCEROS, CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES .. | 324 |
| 4.1.- Localización física de los datos | 325 |
| 4.2.- Transferencias internacionales de datos y <i>Cloud Computing</i> | 327 |
| 4.2.1.- Concepto de transferencia internacional de datos de carácter personal..... | 327 |
| 4.2.2.- Diferencias en las garantías exigidas a las transferencias internacionales, atendiendo al país receptor de los datos personales..... | 328 |
| 4.2.3.- Las transferencias internacionales de datos en el nuevo Reglamento General de Protección de Datos..... | 336 |
| 4.3.- La transferencia de datos personales entre PYMEs españolas y proveedores norteamericanos de <i>Cloud Computing</i> tras la reciente anulación del Acuerdo <i>Safe Harbor</i> por el Tribunal de Justicia de la Unión Europea | 338 |
| 5.- LA IMPORTANCIA DEL CONTRATO ENTRE PROVEEDOR Y CLIENTE. LAS POLÍTICAS DE PRIVACIDAD | 342 |
| 6.- RESPONSABILIDAD POR INCUMPLIMIENTO DE OBLIGACIONES EN MATERIA DE PROTECCIÓN DE DATOS | 345 |
| 7- LOS EFECTOS DE LA FINALIZACIÓN DEL CONTRATO DE COMPUTACIÓN EN LA NUBE SOBRE LOS DATOS PERSONALES | 349 |

ÍNDICE

VOLUMEN II

CAPÍTULO SEXTO. OBLIGACIONES Y RESPONSABILIDADES DE LAS PARTES DEL CONTRATO DE COMPUTACIÓN EN LA NUBE 14

1.- INTRODUCCIÓN 14

2. - EL ACUERDO DE NIVEL DE SERVICIO 16

2.1.- Descripción técnica del acuerdo de nivel de servicio (ANS) y sus parámetros: los objetivos de nivel de servicio (ONS) 17

a) El concepto de acuerdo de nivel de servicio 17

b) Forma y contenido del acuerdo de nivel de servicio 19

2.2.- El tratamiento legal del acuerdo de nivel de servicio 25

3.-OBLIGACIONES DEL PROVEEDOR 27

3.1.- La disponibilidad y su relación con la continuidad de la prestación..... 30

3.2.- La calidad del servicio suministrado (I): el control en el aprovisionamiento de recursos y la adaptabilidad a las necesidades del cliente..... 34

3.2.1. La infraestructura, plataforma y aplicación como productos informáticos y el grado de control de proveedor y cliente sobre ellos 35

3.2.2.- La responsabilidad del proveedor por la adaptabilidad del servicio a las necesidades del cliente y su relación con el deber de información precontractual 39

3.3.-La calidad del servicio (II): la adopción de una política de seguridad adecuada..... 43

3.3.1.- La preservación de la integridad de los datos 43

3.3.2.- La confidencialidad de los datos del cliente y las solicitudes de acceso de terceros 49

3.3.3.- Política de seguridad. Custodia de los datos 54

a) El carácter contractual de la obligación del proveedor de establecer medidas de seguridad 56

b) La seguridad de los sistemas y el plan de emergencia ante incidentes de seguridad como obligaciones de resultado..... 61

c) Responsabilidad en cuanto a la custodia de los datos y pérdidas accidentales 65

3.4- El cumplimiento defectuoso y la determinación de *service credits* como

ÍNDICE

| | |
|--|------------|
| indemnización al cliente | 69 |
| 4.- RESPONSABILIDAD DIRECTA DEL PROVEEDOR: LIMITACIONES Y EXONERACIONES. LA ACEPTACIÓN DE LOS SERVICIOS "TAL CUAL ESTÁN" Y "SEGÚN ESTÉN DISPONIBLES" ("AS IS" Y "AS AVAILABLE") | 75 |
| 4.1.- Las cláusulas limitativas y exoneratorias de responsabilidad y distribución de riesgos entre las partes. Aceptación de los servicios "tal cual están"..... | 75 |
| 4.2.- Límites cuantitativos y temporales a las indemnizaciones por daños y perjuicios..... | 81 |
| 4.3.- La responsabilidad del proveedor por actuaciones de los subproveedores..... | 84 |
| 4.4.- 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 <i>Cloud Computing</i> | 88 |
| 4.4.1.- Cláusulas abusivas y contratos de computación en la nube..... | 89 |
| 4.4.2.- Cláusulas abusivas y pequeños empresarios..... | 90 |
| 5.- OBLIGACIONES DEL SUSCRIPTOR..... | 101 |
| 5.1.- Pago del precio..... | 101 |
| 5.2.- Otras obligaciones del cliente..... | 103 |
| 5.2.1.- La existencia de un deber de colaboración con el proveedor..... | 103 |
| 5.2.2.- Legalidad y pertinencia de los contenidos, cumplimiento de las PUAs, y buena fe contractual..... | 104 |

CAPÍTULO SÉPTIMO. MODIFICACIÓN, SUSPENSIÓN Y EXTINCIÓN DEL CONTRATO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

106

| | |
|--|-----|
| 1.- INTRODUCCIÓN..... | 106 |
| 2.- LA MODIFICACIÓN DE CLÁUSULAS CONTRACTUALES..... | 108 |
| 2.1.- Las modificaciones del servicio y las modificaciones de las condiciones contractuales | 110 |
| 2.2.- La comunicación de las modificaciones. El consentimiento implícito por el uso continuado del servicio..... | 119 |
| 3.- LA SUSPENSIÓN DEL SERVICIO | 122 |
| 3.1.- Las razones de la suspensión del servicio y su validez..... | 122 |
| 3.1.1.- El impago o retraso en el abono de cuotas adeudadas por el cliente | |

ÍNDICE

| | |
|--|-----|
| <i>cloud</i> | 125 |
| 3.1.2.-El incumplimiento de las políticas de uso adecuado..... | 125 |
| 3.1.3.- Las necesidades técnicas..... | 126 |
| 3.1.4.- Otras causas..... | 127 |
| 3.2.- El procedimiento de suspensión unilateral | 128 |
| 3.3.- Las consecuencias de la suspensión del servicio para el cliente..... | 130 |
| 4.- LA EXTINCIÓN DEL CONTRATO..... | 132 |
| 4.1.- Las causas de terminación del contrato de computación en la nube en las cláusulas resolutorias..... | 134 |
| 4.1.1.- El desistimiento unilateral..... | 135 |
| 4.1.2.- La resolución del contrato por incumplimiento de una de las partes... | 138 |
| 4.1.3.- La imposibilidad sobrevenida de continuar con la prestación del servicio..... | 141 |
| 4.2.- Efectos de la extinción del contrato de computación en la nube..... | 142 |
| 5.- LA RECUPERACIÓN DE LOS CONTENIDOS ALOJADOS EN LA NUBE POR EL CLIENTE Y SU PORTABILIDAD A OTRO PROVEEDOR <i>CLOUD</i> | 143 |
| 5.1.-La portabilidad de los datos y la portabilidad de las aplicaciones..... | 145 |
| 5.2.- La expectativa de recuperación de los datos..... | 148 |
| 5.2.1.- La retención de contenidos por parte del proveedor y su relación con la contraprestación económica del servicio <i>cloud</i> | 149 |
| 5.2.2.- La retención de contenidos por parte del proveedor y su relación con la causa de extinción del contrato..... | 150 |
| 5.2.3.- El derecho a la recuperación de los datos y a la portabilidad..... | 154 |
| 5.2.4.- La asistencia al cliente durante el tránsito de los datos a un tercer proveedor. El plazo para la recuperación de los datos..... | 160 |
| 6.-LA PRESERVACIÓN DE LOS CONTENIDOS Y SU BORRADO UNA VEZ EXTINGUIDA LA RELACIÓN CONTRACTUAL..... | 163 |
| 6.1.- La preservación de los contenidos del cliente tras finalizar la prestación.. | 164 |
| 6.2.-Las técnicas de borrado de contenidos en la computación en la nube y sus garantías..... | 169 |
| 6.2.1.- Los diferentes niveles de borrado de los datos..... | 169 |
| 6.2.2.- Algunas medidas relacionadas con el borrado: la cláusula de confidencialidad, la anonimización y la seudonimización | 171 |
| a) La cláusula de confidencialidad..... | 172 |

ÍNDICE

| | |
|---|-----|
| b) La anonimización de información personal..... | 173 |
| c) La seudonimización de información personal..... | 177 |
| 6.2.3.- La prueba del borrado de datos..... | 182 |
| 6.3.- El borrado de datos como obligación del proveedor | 183 |

CAPÍTULO OCTAVO. LA CONTRATACIÓN DE SERVICIOS DE COMPUTACIÓN EN LA NUBE POR EL PEQUEÑO EMPRESARIO TURÍSTICO.....

| | |
|--|------------|
| TURÍSTICO..... | 189 |
| 1.- INTRODUCCIÓN..... | 189 |
| 2.- LA UTILIDAD DEL <i>CLOUD COMPUTING</i> EN EL SECTOR TURÍSTICO..... | 193 |
| 2.1.- Almacenamiento remoto de archivos y copias de seguridad..... | 194 |
| 2.2.- Correo electrónico y <i>suites</i> ofimáticas en la nube..... | 195 |
| 2.3.- Sistemas de gestión de recursos empresariales (<i>Enterprise Resource Planning</i> o ERP) | 197 |
| 2.4.- Sistemas de gestión de clientes (<i>Customer Relationship Management</i> o CRM)..... | 199 |
| 2.5.- Sistemas de gestión de la reputación <i>online</i> (<i>Online Reputation Management</i> u ORM)..... | 199 |
| 2.6.- Alojamiento de páginas web en la nube o <i>Cloud Hosting</i> | 200 |
| 2.7.- Otros usos de la computación en la nube en el sector turístico..... | 201 |
| 3.- LA PROBLEMÁTICA JURÍDICA DEL <i>CLOUD COMPUTING</i> ESPECÍFICA DE SERVICIOS DESTINADOS AL SECTOR TURÍSTICO..... | 203 |
| 3.1.- El objeto del contrato predispuesto: ¿cesiones de licencia de software o servicios de computación en la nube?..... | 204 |
| 3.2.- Imposibilidad de negociación contractual..... | 205 |
| 3.3.- Limitación y exclusión de responsabilidades..... | 206 |
| 3.4.- La intermediación. El socio o " <i>partner</i> " del proveedor..... | 209 |
| 3.5.- La disponibilidad del servicio y su relevancia en picos de demanda estacionales..... | 210 |
| 3.6.- Suspensión y terminación del contrato. Efectos..... | 213 |
| 4.- LA PROTECCIÓN DE DATOS PERSONALES APLICADA A PEQUEÑOS EMPRESARIOS DEL SECTOR TURÍSTICO USUARIOS DE SERVICIOS | |

ÍNDICE

| | |
|--|------------|
| <i>CLOUD</i> | 214 |
| 4.1.- El pequeño empresario turístico como responsable del tratamiento. La importancia de la finalidad del tratamiento y del consentimiento previo e informado.. | 215 |
| 4.2.- La transmisión de datos personales a terceros a través de servicios <i>cloud</i> .. | 219 |
| 4.3.- Transferencias internacionales de datos personales..... | 220 |
| 4.4.- Referencias en el documento de seguridad a los sistemas <i>cloud</i> | 221 |
| 4.5.- Destrucción, inhabilitación o borrado de información personal almacenada en la nube..... | 223 |
| 5.- WEB 2.0 EN EL SECTOR TURÍSTICO: ASPECTOS JURÍDICOS ANÁLOGOS A LA CONTRATACIÓN DE SERVICIOS <i>CLOUD</i> | 225 |
| 5.1.- Los términos de uso del buscador o comparador. Aspectos jurídicos análogos al <i>Cloud Computing</i> | 225 |
| 5.1.1.- Políticas de uso adecuado y veracidad de los contenidos compartidos por el usuario..... | 226 |
| 5.1.2.- Propiedad intelectual de los contenidos creados por el usuario..... | 228 |
| 5.1.3.- Limitaciones y exclusiones de responsabilidad..... | 228 |
| 5.2. Problemas específicos entre las plataformas Web 2.0 y el pequeño empresario turístico..... | 232 |
| 5.2.1.- La reputación corporativa <i>online</i> | 232 |
| 5.2.2.- La salida de la empresa turística de la plataforma Web 2.0..... | 234 |
| 6.- CONCLUSIONES Y RECOMENDACIONES AL PEQUEÑO EMPRESARIO DEL SECTOR TURÍSTICO SUScriptor DE SERVICIOS <i>CLOUD</i> | 237 |
| | |
| CONCLUSIONES FINALES | 239 |
| BIBLIOGRAFÍA | 255 |

OBLIGACIONES Y RESPONSABILIDADES DE LAS PARTES DEL CONTRATO DE COMPUTACIÓN EN LA NUBE

1.- INTRODUCCIÓN

El núcleo de la relación jurídica entre el prestador de servicios y el cliente se manifiesta en sus diferentes obligaciones contractuales. Algunas veces se acuerdan mediante la negociación entre las partes. En otras ocasiones, como sucede con los contratos objeto de este trabajo, el cliente se adhiere a las condiciones predispuestas por el proveedor de servicios de computación en la nube pública.

El contenido de estas obligaciones es heterogéneo, ya que dependerá, en primer lugar, de la configuración concreta del tipo de servicio prestado (esto es, de la infraestructura, plataforma o software como servicios), en segundo lugar, de la delimitación de tareas y responsabilidades que, a su criterio, configure cada proveedor, y, por último, de la tipología de cliente al cual se dirige la oferta, puesto que existirán obligaciones que se manifestarán con distinta intensidad en contratos con consumidores y en contratos suscritos por pequeños y medianos empresarios. Igualmente, ocurre que algunas cláusulas incorporadas en el contrato resultan ser un mero reflejo de obligaciones establecidas legalmente¹.

El análisis de los distintos clausulados contractuales utilizados en la práctica demuestra que existen gradaciones tanto en la distribución de responsabilidades entre las partes como en el establecimiento de compensaciones. Tras comparar

1 Por ejemplo, la inclusión en las políticas de uso de cláusulas relativas al uso del servicio *cloud* para actividades ilícitas, o el recordatorio sobre posibles infracciones de derechos de propiedad intelectual.

CAPÍTULO SEXTO

diferentes contratos de servicios de *Cloud Computing*, se evidencia cómo algunos proveedores se muestran reacios a asumir ciertas obligaciones ante el cliente, como sucede con los servicios no retribuidos monetariamente² o con sede fuera de la Unión Europea³.

Del mismo modo, para que exista una relación correcta y adecuada que satisfaga las necesidades de las partes, serán necesarios deberes de colaboración recíproca. El deber de información, por una parte, es predicable del proveedor del servicio en cuanto a aquello que suministra, las contraprestaciones que exige a cambio y la disponibilidad del suministro, así como eventuales incidencias que puedan tener lugar durante la prestación⁴. Por otra parte, será recomendable que el cliente profesional suscriptor de servicios *cloud*, en su propio beneficio, ponga en conocimiento del proveedor aspectos sobre sus necesidades particulares y expectativas, con el fin de obtener la máxima adecuación entre lo ofertado por el proveedor y la particular operativa empresarial del cliente. Además, el cliente deberá cumplir con la política de uso del servicio, y asegurarse de que el contrato suscrito le permite satisfacer todas las exigencias legales que recaen sobre sus espaldas, especialmente, aquellas cuyo incumplimiento pueda ocasionarle sanciones económicas u obligaciones de indemnizar a terceros.

En este capítulo estudiaremos el entramado de obligaciones derivadas de las cláusulas de contratación de servicios de computación en la nube y veremos cómo se armonizan en la práctica los intereses del cliente (esto es, la búsqueda de la mejor relación calidad-legalidad-precio) con la pretensión del proveedor de la máxima

2 Si bien resulta razonable que los servicios sujetos a precio ofrezcan mayores garantías y compromiso por parte del proveedor que aquellos que se ofrecen al cliente sin contraprestación dineraria, algunos proveedores parecen escudarse en esa falta de remuneración dineraria para excluir responsabilidades, algunas de ellas derivadas de obligaciones inherentes a la propia naturaleza del contrato. Consideramos que sería discutible la admisibilidad de ciertas exclusiones de responsabilidad o el incumplimiento de los compromisos en cuanto a la calidad de la prestación del servicio en aquellos casos en los cuales el proveedor obtiene igualmente un beneficio económico, como puede suceder cuando se exige del cliente que facilite datos personales u otra información sobre su comportamiento (siempre y cuando no sean necesarios para la prestación ordinaria del servicio), o que ceda derechos al proveedor.

3 BRADSHAW, S; MILLARD, C; WALDEN, I, "*Standard contracts for Cloud Services*", *Cloud Computing Law*, (Coord. Christopher Millard), 1ª edición, Oxford, 2013, págs. 58 y ss.

4 En relación al término "suministro" y derivados, que aparecen en este capítulo, queremos puntualizar que su uso se realiza como referencia a la forma en la cual tiene lugar la prestación, como acceso a recursos remotos que se proporcionan a través de la Red global. En ningún modo se identifica el contrato de computación en la nube como un contrato de naturaleza jurídica coincidente con el suministro eléctrico o de otros bienes. Para más detalle, ver capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

CAPÍTULO SEXTO

rentabilidad del negocio, así como las responsabilidades que pueden derivarse de su incumplimiento. Recordemos que el objeto de esta tesis está dedicado a contratos de nube pública no negociables suscritos por pequeños empresarios⁵.

2.- EL ACUERDO DE NIVEL DE SERVICIO (ANS)

Según la definición que el *National Institute of Standards and Technology* (NIST) realiza de la computación en la nube, mencionada en anteriores capítulos⁶, una de las principales características de este entorno consiste en proporcionar acceso al usuario a recursos computacionales que se le asignan de manera automatizada y bajo demanda, a través de Internet⁷.

Dependiendo del servicio, estos recursos computacionales podrán ser de distinta naturaleza: redes virtuales, capacidad de procesamiento o almacenamiento (IaaS o infraestructura como servicio), plataformas para desarrollo de software (PaaS o plataforma como servicio) o aplicaciones informáticas (SaaS o software como servicio)⁸. El cliente suscriptor de estos servicios tendrá unas expectativas de la prestación, y el proveedor puede comprometerse a prestar el servicio según ciertos niveles u objetivos referenciados en el contrato suscrito, con el fin de cubrir las expectativas generadas en el cliente.

Los objetivos de prestación de un servicio *cloud* pueden variar considerablemente según sean prestados por uno u otro prestador. Tanto su adopción como su contenido dependerán del criterio del proveedor, de acuerdo con la tecnología de la que dispone y de su estrategia empresarial. También será relevante si el servicio se presta o no con sujeción a una contraprestación dineraria por parte del cliente, puesto que, en general, se cumple la regla de que "a mayor precio, mayor compromiso asumido el proveedor".

Estos objetivos de prestación, denominados objetivos de nivel de servicio o

5 En concepto de "pequeño empresario" que aparece en este capítulo abarca también a profesionales independientes, así como a medianos empresarios que carezcan de posibilidad de negociación de las cláusulas contractuales de contratos de adhesión predispuestos por proveedores de computación en la nube y que se encuentren en una situación de desequilibrio contractual similar a la del pequeño empresario.

6 Ver apartado "Características de la computación en la nube", en el capítulo "Concepto y características técnicas de la computación en la nube".

7 MARTÍNEZ MARTÍNEZ, Ricard, "El Derecho y el *Cloud Computing*", *Derecho y Cloud Computing* (Coord. Ricard Martínez), Pamplona, 2012, pág. 16.

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

CAPÍTULO SEXTO

Service Level Objectives (en adelante, también ONS), pueden afectar a diferentes características de la prestación (seguridad, disponibilidad, custodia y manejo de datos, etc), representarse a través de diferentes medidas o parámetros, y asociarse o no a compensaciones en favor del cliente. Asimismo, suelen aparecer recogidos en los llamados acuerdos de nivel de servicio o *Service Level Agreements* (en adelante, también ANS). A continuación, nos detendremos en el estudio de su concepto y configuración jurídica.

2.1.- Descripción técnica del acuerdo de nivel de servicio y sus parámetros: los objetivos de nivel de servicio

En este apartado analizaremos algunas cuestiones derivadas del contenido de los acuerdos de nivel de servicio o *Service Level Agreements* (en adelante, también ANS) que se integran en contratos de nube pública no negociables⁹.

2.1.1.- El concepto de acuerdo de nivel de servicio

Desde el punto de vista técnico, el estándar ISO 20000-1:2011¹⁰ definió el acuerdo de nivel de servicio como "el acuerdo documentado entre el proveedor y el cliente que identifica los servicios y los objetivos del servicio. Puede estar incluido en un contrato o en otro tipo de acuerdo documentado"¹¹.

La finalidad de cualquier acuerdo de nivel de servicio es la de objetivizar, a través de definiciones, parámetros, estándares u otras referencias, todo o parte del deber de diligencia del proveedor, y no siempre llevará asociadas compensaciones económicas. Por otra parte, puede incluir otros contenidos que, igualmente, den concreción contractual al impreciso concepto de diligencia profesional del

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

10 Definición del acuerdo de nivel de servicio adoptada por el estándar ISO /IEC 20000-1:2011 en relación a los servicios de administración de sistemas: "Documented agreement between the service provider and customer that identifies services and service targets. (...) A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier. (...) A service level agreement can be included in a contract or another type of documented agreement". Disponible en: <http://www.iso.org/iso/catalogue_detail?csnumber=51986>. [Fecha de consulta: 14 de noviembre de 2016]. Esta definición ha sido referenciada dentro del estándar ISO 17788/2014 sobre conceptos y vocabulario aplicables a los servicios de computación en la nube.

11 Queremos puntualizar que, en el caso de los contratos de adhesión, el acuerdo de nivel de servicio (ANS) no ha sido específicamente negociado o acordado, sino que el cliente se ha adherido a las condiciones generales facilitadas por el proveedor de servicios, entre las cuales, además de otras estipulaciones, se hallan los compromisos sobre los parámetros de desempeño del servicio *cloud*.

CAPÍTULO SEXTO

proveedor, como la descripción del servicio que se presta¹².

Entenderemos, pues, que el acuerdo de nivel de servicio recoge cualesquiera propósitos a los cuales se compromete el proveedor relacionados con la prestación del servicio, como por ejemplo los niveles de seguridad que pueda garantizar a través de la adopción de estándares de seguridad, los tiempos previstos para la recuperación de datos por el cliente, la realización de copias de seguridad, la localización de los datos en determinadas ubicaciones geográficas o los compromisos sobre el tratamiento y usos de los datos personales.

Al respecto cabe destacar que la Comisión Europea, consciente de la naturaleza global de la computación en la nube y de la complejidad de algunos acuerdos de nivel de servicio dependiendo del tipo de implementación y del modelo de servicio *cloud* prestado, publicó el documento *Cloud Service Level Agreement Standardisation Guidelines*, que establece conceptos y definiciones que pueden usarse para crear acuerdos de nivel de servicio que se incluyan en contratos y que ha servido para elaborar el estándar ISO 19086-1:2016¹³.

12 Este trabajo se enmarca dentro de la segunda acción clave de la *Cloud Computing Strategy*, denominada *Development of model safe and fair contract terms*, y destinada al desarrollo de cláusulas modelo equitativas para contratos entre proveedores *cloud* y clientes (no solo consumidores). Dentro de esta misma acción clave se encuentra la tarea de realizar un código de conducta para proveedores *cloud*, y cuyo desarrollo en el momento de realización de este trabajo aún no ha finalizado. En el mismo sentido acoge el concepto de "acuerdo de nivel de servicio" el considerando 18 de 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: "(...) Para algunos contenidos digitales, es habitual que los proveedores describan, en un acuerdo de nivel de servicios, el servicio y los objetivos del servicio mensurables (...)". Los contratos de *Cloud Computing* suscritos por consumidores se encuentran incluidos dentro de su ámbito material de aplicación, al entenderse dentro del apartado b) del concepto de "contenidos digitales" recogido por la propia Propuesta: "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". Sin embargo quedarían fuera de su regulación, en principio, los contratos de *Cloud Computing* suscritos por pequeños empresarios.

13 El documento del subgrupo de expertos en acuerdos de nivel de servicio de la *Cloud Computing Strategy* se publicó el 24 de junio de 2014. Este documento sirvió de referencia para la elaboración del estándar ISO 19086-1:2016. *Cloud Service Level Agreement Standardisation Guidelines* [en línea]. Disponible en: <<https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>>. *ISO19086-1:2016 Information technology-Cloud Computing- SLA framework- Part 1- Overview and concepts*. Disponible en: <<https://www.iso.org/standard/67545.html>>. [Fecha de consulta: 18 de mayo de 2017].

CAPÍTULO SEXTO

2.1.2.- Forma y contenido del acuerdo de nivel de servicio

El acuerdo de nivel de servicio (o ANS) integrado dentro de los contratos de servicios *cloud* frecuentemente se recoge en las propias condiciones generales o en un anexo separado. Jurídicamente, resulta irrelevante la forma en la cual se recoja, porque se trata de acuerdos que generan obligaciones y otros efectos jurídicos para las partes¹⁴. Suele contener:

1) la descripción específica del servicio o servicios proporcionados por el proveedor¹⁵;

2) los parámetros u objetivos de prestación del servicio a los que se compromete el proveedor, es decir, los objetivos de nivel de servicio u ONS y sus indicadores o referentes técnicos¹⁶, y

3) las compensaciones en caso de incumplimiento de estos objetivos mínimos, a menudo dispuestas a modo de créditos de servicio (*service credits*¹⁷).

Los acuerdos de nivel de servicio pueden configurar como objetivos diferentes parámetros de prestación. Sin embargo, en nuestra opinión, es más apropiado calificarlos como mínimos, puesto que si no se consiguen estos mínimos, se pueden devengar compensaciones en favor del cliente por el cumplimiento

14 Así lo reconoce el considerando 18 de 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: "(...) Estos acuerdos de nivel de servicios se presentan generalmente como anexos al contrato principal y son un componente importante de la relación contractual entre el proveedor y el consumidor". Recordemos que esta Propuesta de Directiva únicamente rige en contratos suscritos por consumidores.

15 Dependiendo del tipo de servicio *cloud* prestado y del proveedor que los predisponga, los ANS pueden variar considerablemente. Esta es una de las motivaciones que impulsa a la *European Cloud Computing Strategy* a adoptar estas Directrices en relación a los estándares de los ANS, con el fin de homogeneizar los términos existentes entre los diferentes ANS y facilitar al cliente *cloud* la toma de decisiones. Así lo afirma en su preámbulo en su documento *Cloud Service Level Agreement Standardisation Guidelines*: "Furthermore different cloud services and deployment models will require different approaches to SLAs, adding to the complexity of SLAs. Finally, SLA terminology today often differs from one cloud service provider to another, making it difficult for cloud service customers to compare cloud services". *Cloud Service Level Agreement Standardisation Guidelines*, [en línea]. Disponible en: <<https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>>. [Fecha de consulta: 14 de noviembre de 2016]. Ver apartado "La responsabilidad del proveedor por la adaptabilidad del servicio y su relación con el deber de información precontractual", en este mismo capítulo.

16 Estos parámetros suelen variar dependiendo del servicio prestado (software como servicio de almacenamiento remoto, software como servicio de aplicaciones informáticas, plataforma como servicio, etc.).

17 *Service credit*. Compensaciones predeterminadas que permiten al cliente una rebaja en futuras facturaciones por no alcanzarse unos mínimos acordados contractualmente. (Definición propia).

CAPÍTULO SEXTO

defectuoso del servicio¹⁸. Así, estos mínimos contractuales son verdaderas obligaciones contractuales a las cuales se compromete el proveedor, y por tanto, el cliente suscriptor debería tener derecho a ser compensado (art. 1101 del Código Civil)¹⁹. No obstante, como veremos en posteriores apartados, para que esta compensación en favor del pequeño empresario realmente surja efecto, deberemos estar a las exenciones de responsabilidad del proveedor que el pequeño empresario haya podido aceptar al suscribir el contrato.

Los parámetros u objetivos de nivel de servicio (en adelante, también ONS), pueden clasificarse en²⁰:

1) Objetivos de nivel de servicio sobre el desempeño del servicio *cloud* y del funcionamiento de la interfaz entre el proveedor y el cliente: el tiempo de respuesta del sistema las peticiones del cliente²¹, la capacidad máxima del sistema *cloud*²², la

18 Ver apartado "El cumplimiento defectuoso y la determinación de *service credits* como indemnización al cliente", en este mismo capítulo.

19 Artículo 1101 del Código Civil: "Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas. "

20 Siguiendo la clasificación que efectúan las directrices elaboradas por el *Cloud Select Industry Group*, que integra a miembros de la industria de la computación en la nube como Microsoft, IBM o la *Cloud Security Alliance*, y publicadas por la Comisión Europea, en el documento *Cloud Service Level Agreement Standardisation Guidelines* [en línea]. Disponible en: <<https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>>. [Fecha de consulta: 14 de noviembre de 2016].

21 El tiempo de respuesta comprende el intervalo entre que el cliente del servicio *cloud* inicia una petición (estímulo) y el sistema del proveedor inicia una acción en respuesta a ese estímulo. Este ONS puede variar dependiendo del punto en el cual se inicia la medición. Por ejemplo, esta medición puede iniciarse desde que el cliente inicia el estímulo en su dispositivo, o, en cambio, desde que el estímulo llega al sistema del proveedor y se produce la respuesta. En el primer caso, se estará considerando también el tiempo de tránsito durante el cual el estímulo viaja a través de la red y que escapa del control del proveedor. Además, en relación con este objetivo, son importantes los parámetros de "tiempo medio de respuesta" (media estadística sobre la respuesta que observa un servicio *cloud* en relación con una determinada petición) y "tiempo máximo de respuesta" (objetivo máximo de tiempo de respuesta ante una determinada petición). COMISIÓN EUROPEA, *Cloud Service Level Agreement Standardisation Guidelines*, *op. cit.*, pág. 16.

22 Capacidad máxima del sistema. Este parámetro determina la capacidad del sistema *cloud* en relación a alguna o a varias de sus características técnicas, como el número de conexiones simultáneas que puede soportar, el número máximo de usuarios que pueden estar conectados a la vez, el número de recursos máximos (almacenamiento, memoria, rendimiento de los procesadores, etc.). Una de las ventajas de los sistemas *cloud* es, como hemos mencionado en el capítulo primero de este trabajo, la escalabilidad, que permite al cliente aumentar el límite de estas capacidades, realizando cambios en la suscripción del servicio. COMISIÓN EUROPEA, *Cloud Service Level Agreement Standardisation Guidelines*, *op. cit.*, pág. 16.

CAPÍTULO SEXTO

conectividad externa²³, las interfaces de soporte²⁴, compromisos adoptados en relación a la terminación del contrato²⁵, la interoperabilidad de las aplicaciones²⁶, etc.

2) Objetivos de nivel de servicio sobre seguridad del sistema²⁷: confiabilidad del servicio, mecanismos de autenticación y autorización a usuarios, uso de criptografía, manejo de incidentes de seguridad, monitorizaciones, auditorías de seguridad, detección y corrección de vulnerabilidades, etc.

3) Objetivos de nivel de servicio sobre seguridad de los datos migrados²⁸: latencia del replicado, frecuencia y métodos de realización de copias de seguridad por el proveedor, tiempo de recuperación de los datos desde la copia de seguridad, borrado y portabilidad de datos²⁹, etc.

4) Objetivos de nivel de servicio sobre tratamiento de datos de carácter personal y de datos migrados por el cliente³⁰: especificación de aquellas finalidades

23 Conectividad Externa. Potencial del servicio *cloud* para conectarse a sistemas externos al propio servicio (como pueden ser los dispositivos informáticos del cliente) así como a otros servicios *cloud*, o para sincronizarse con estos. COMISIÓN EUROPEA, *Cloud Service Level Agreement Standardisation Guidelines, op. cit.*, pág. 17.

24 Interfaces de soporte. El proveedor puede comprometerse a mantener una interfaz de soporte para responder a problemas o a dudas del cliente. Por ejemplo, pueden aparecer ONS en cuanto a horarios de atención a dudas, tiempos de respuesta a consultas efectuadas por el cliente, o tiempos máximos de reacción ante peticiones relacionadas la seguridad. COMISIÓN EUROPEA, *Cloud Service Level Agreement Standardisation Guidelines, op. cit.*, pág. 18.

25 Compromisos relacionados con la terminación del contrato. Puede incluir ONS como el tiempo del cual dispone el cliente para obtener del proveedor una copia de sus datos (período de recuperación de datos), el tiempo durante el cual el proveedor se compromete a retener copias de seguridad una vez terminado el contrato (período de retención de datos) o la descripción de los datos derivados del servicio que conservará el proveedor una vez extinguida la relación contractual (retención de datos residuales). COMISIÓN EUROPEA, *Cloud Service Level Agreement Standardisation Guidelines, op. cit.*, pág. 16.

26 Interoperabilidad. Puede entenderse como "La habilidad de dos o más sistemas o aplicaciones para intercambiar información y utilizar recíprocamente la información intercambiada". Traducción propia de la definición original recogida por la ISO/IEC 17788:2014: "The ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged". Disponible en: <http://www.iso.org/iso/catalogue_detail?csnumber=60544> [Fecha de consulta: 14 de noviembre de 2016].

27 Ver apartado "La calidad del servicio suministrado: la adaptabilidad a las necesidades del cliente y la adopción de una política de seguridad adecuada", en este mismo capítulo.

28 Ver apartado "La calidad del servicio suministrado: la adaptabilidad a las necesidades del cliente y la adopción de una política de seguridad adecuada", en este mismo capítulo.

29 Ver 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".

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

CAPÍTULO SEXTO

del tratamiento que excedan de las necesarias para la prestación del servicio (por ejemplo, elaborar perfiles de usuarios, personalizar publicidad, etc.) y que permiten al proveedor *cloud* calificarlo como responsable del tratamiento realizado para estas finalidades; localizaciones geográficas en las cuales pueden albergarse y/o tratarse los datos del cliente; tiempo de retención de los datos del cliente antes de ser borrados; número o lista de subcontratistas relacionados con el tratamiento de datos personales de clientes del servicio *cloud*; política de recuperación de datos en caso de desastre; documentación a disposición de interesados respecto del cumplimiento de obligaciones en materia de protección de datos, notificaciones de brechas de seguridad, estándares y certificados de cumplimiento con los cuales se compromete el proveedor³¹; tiempo de respuesta ante peticiones realizadas por el empresario cliente para que pueda atender, como responsable, a los derechos de los titulares de datos personales; etc. Cabe decir que estas medidas pueden tratarse a modo de objetivo de nivel de servicio, es decir, como objetivos que el proveedor debe alcanzar. Otras obligaciones y responsabilidades podrán asumirse a través de otros mecanismos, como la adhesión a códigos de conducta, certificaciones de cumplimiento de estándares en materia de protección de datos, o mediante otras disposiciones incluidas en el contrato, o a través de la aplicación directa de la normativa sobre privacidad.

En la práctica contractual, los proveedores *cloud* utilizan con frecuencia diferente terminología, y no existe homogeneidad entre el contenido de las diferentes referencias y conceptos técnicos que determinan estos parámetros, lo cual dificulta la comparación de servicios por parte de los clientes de los servicios y crea inseguridad jurídica y falta de confianza en los sistemas de computación en la nube³².

La Comisión Europea ha realizado múltiples avances en cuanto a esta homogeneización de estándares dentro de la industria de la computación en la nube. La mayor parte de ellos han tenido lugar dentro del conjunto de acciones previstas

31 Ver apartado "El tratamiento legal del acuerdo de nivel de servicio", en este mismo apartado.

32 Así se recoge en la Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, Al Comité Económico y Social y al Comité de las Regiones COM (2012) 529 final, pág. 9, titulado "*Unleashing the potential of Cloud Computing in Europe*": "There is a need for a chain of confidence-building steps to create trust in cloud solutions. This chain starts with the identification of an appropriate set of standards that can be certified in order to allow public and private procurers to be confident that they have met their compliance obligations and that they are getting an appropriate solution to meet their needs when adopting cloud services. These standards and certificates in turn can be referenced in terms and conditions so that providers and users feel confident that the contract is fair. The preparatory work mentioned above indicates the need for specific frameworks for Cloud Computing in relation to both standards and certification and contract terms and conditions".

CAPÍTULO SEXTO

por la *European Cloud Computing Strategy*, adoptada por la Comisión Europea en 2012, en el marco de la Agenda Digital Europea³³.

En el informe final publicado en 2013 que resultó de la primera fase para la coordinación de estándares (*Cloud Standard Coordination*), en el ámbito de la mencionada *European Cloud Computing Strategy*, se estableció la importancia de los acuerdos de nivel de servicio en tres momentos de la relación contractual entre el

33 En primer lugar, se identificó la necesidad de adoptar estándares técnicos en áreas como la seguridad, la interoperabilidad o la portabilidad, que resultan cruciales para la expansión y desarrollo de los servicios de computación en la nube, así como certificaciones de autoridades reguladoras respecto de su cumplimiento, como parte de la propia estrategia. Así se afirma en la Comunicación de la Comisión al Parlamento Europeo, el Consejo, el Comité Económico y Social y el Comité de las Regiones, de 27 de septiembre de 2012 COM (2012) 529 final, titulada *Unleashing the Potential of Cloud Computing in Europe*. (Disponible en la web de la Unión Europea. <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>>). Posteriormente, con la colaboración del *European Telecommunications Standards Institute* (ETSI), se llevó a cabo la *Cloud Standards Coordination*. Tales trabajos de coordinación, tuvieron lugar en dos fases. La primera de ellas finalizó en noviembre de 2013 con la publicación del informe *Cloud Standards Coordination Final Report* [en línea]. Disponible en: <http://csc.etsi.org/resources/CSC-Phase-1/CSC-Deliverable-008-Final_Report-V1_0.pdf>. La segunda fase de la *Cloud Standards Coordination* se ha centrado en cuatro aspectos esenciales para la coordinación de estándares: entender las necesidades del cliente, estándares y código abierto, la interoperabilidad y la conformidad respecto de la seguridad, y recopilación y valoración de estándares y especificaciones propuestos por las diferentes organizaciones de estandarización. En enero de 2016 se publicaron los diferentes informes con las conclusiones al respecto. Están disponibles en: <<http://csc.etsi.org/phase2.html>>. [Fecha de consulta: 18 de noviembre de 2016]. Por otra parte, en 2014, presentó las *Directrices para la estandarización de los acuerdos de nivel de servicio en el sector de la computación en la nube*, dentro de la *European Cloud Computing Strategy*. Estas directrices fueron elaboradas por el subgrupo de trabajo en acuerdos de nivel de servicio del *Cloud Select Industry Group* (C-SIG SLA), que integra a representantes de la industria del *Cloud Computing*, con el fin de ayudar a los usuarios empresariales de servicios de computación en la nube a entender las áreas críticas de la computación en la nube y a aumentar la transparencia de las prácticas contractuales para así incrementar la confianza en la nube. En el preámbulo de estas Directrices se afirma que los acuerdos de nivel de servicio son un componente esencial de la relación contractual entre proveedor y cliente, y que debido a la naturaleza de los servicios *cloud*, la estandarización de los contenidos del acuerdo de nivel de servicio mejorará la comprensión y la claridad de estos acuerdos. Según las mencionadas Directrices, los objetivos de nivel de servicio deberían servir para ilustrar y especificar conceptos técnicos comprensibles para empresarios suscriptores y demás interesados, puesto que son los compromisos que asume el proveedor *cloud* como prestador de un servicio de calidad (pág. 8). En efecto, la proliferación de referencias o estándares de seguridad y prestación diferentes, adoptados por los distintos proveedores e instituciones (pág. 8), derivan en la falta de certeza sobre cuáles de ellos pueden ofrecer un nivel de calidad apropiado a las necesidades del cliente. *Cloud Service Level Agreement Standardisation Guidelines*" (Directrices para la estandarización de los acuerdos de nivel de servicio en el sector de la computación en la nube. Traducción propia) [en línea]. Disponible en: <<https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>>. [Fecha de consulta: 14 de noviembre de 2016].

CAPÍTULO SEXTO

cliente y el proveedor de servicios de computación en la nube³⁴. En la etapa precontractual, el ANS sirve para poner en conocimiento del cliente los requisitos técnicos y operativos del servicio *cloud*, permitiéndole comparar con otros prestadores del servicio *cloud* y orientándole sobre la adecuación del servicio a sus necesidades empresariales. En la etapa de ejecución de la prestación, el ANS permite que los objetivos de nivel de servicio establecidos sirvan de referencia a la hora de asegurar la calidad de la prestación y adoptar medidas correctoras si los objetivos de nivel de servicio no se cumplen. Por último, en la fase de terminación del contrato las partes pueden hacer uso del ANS para evaluar si el servicio se ha incumplido o aclarar discrepancias respecto de devoluciones al cliente de datos migrados y borrado de datos remanentes en los sistemas del proveedor.

Como reconoce el mismo informe, para que el ANS sea verdaderamente eficiente, es esencial que los objetivos de nivel de servicio que contiene:

a) estén bien definidos, es decir, que los proveedores no puedan interpretar las medidas de manera diferentes, ya que ello obstaculizaría la pretendida objetividad de los ONS como medidas de referencia y obstaculizaría al cliente comparar entre diferentes servicios;

b) estén determinados, es decir, que las medidas establecidas para medir los aspectos técnicos del servicio no puedan generar resultados aleatorios, siendo recomendable dar homogeneidad a las medidas referentes a los mismos aspectos técnicos que operan en sistemas de computación en la nube prácticamente idénticos;

c) muestren la correlatividad entre los objetivos de nivel de servicio y el valor del servicio percibido por el cliente, es decir, el cliente debe poder comprender la utilidad de ese objetivo, y para ello debe ser puesto en relación con el desempeño práctico de la prestación (por ejemplo, la medida de la velocidad de procesamiento del sistema *cloud*, establecida de manera abstracta no será útil para el cliente, sino que debe relacionarse con la eficacia y funcionalidad de las tareas que puede llevar a cabo el cliente en los sistemas del proveedor);

d) sean comparables, es decir, que los diferentes parámetros presentados por los proveedores permitan conocer los aspectos más importantes de la prestación de los servicios, para que el cliente pueda decidir de manera informada entre todas las propuestas de servicios *cloud* examinadas provenientes de distintos proveedores.

34 ETSI, *Cloud Standards Coordination Final Report, november 2013, version 1.0* [en línea], págs. 6, 7. Disponible en: <http://csc.etsi.org/resources/CSC-Phase-1/CSC-Deliverable-008-Final_Report-V1_0.pdf>. [Fecha de consulta: 21 de noviembre de 2016]

CAPÍTULO SEXTO

Por último, queremos adelantar que, cuando el contrato no establezca compensaciones por no cumplirse los objetivos de nivel de servicio (a modo de créditos de nivel de servicio u otros mecanismos similares), deberemos estar a la distribución de riesgos recogida contractualmente para saber si el cliente pequeño empresario tiene o no derecho a ser compensado, ya que puede haber renunciado a este derecho mediante cláusulas limitativas o exclusivas de la responsabilidad del proveedor. A nuestro parecer, los pequeños empresarios en muchos casos se ven injustamente desamparados ante incumplimientos de la relación contractual, con lo cual consideramos que deberían ser protegidos de tales contenidos abusivos³⁵.

2.2.-El tratamiento legal del acuerdo de nivel de servicio

Como se ha mencionado en el anterior apartado, el acuerdo de nivel de servicio (ANS) incluye obligaciones relacionadas con diferentes aspectos contractuales (seguridad, conservación de datos del cliente, desempeño de la prestación, etc.), muchas de ellas a modo de obligaciones de medios y en atención a su deber de diligencia profesional.

Sin embargo, aunque los objetivos de nivel de servicio u ONS (es decir, aquellos factores que puede incluir el acuerdo de nivel de servicio, que concretan aspectos genéricos mensurables y respecto de los cuales el proveedor manifiesta prestar unos mínimos) son susceptibles de considerarse obligaciones de resultado³⁶, coincidimos con algunos autores en que estos niveles de calidad en la prestación de servicios de computación en la nube no implican una obligación para el proveedor respecto de la obtención de un resultado concreto, sino que constituyen meros criterios de medición del grado de cumplimiento de su obligación³⁷. Por ello, no

35 Ver apartados "El cumplimiento defectuoso y la determinación de *service credits* como indemnización al cliente", y "Responsabilidad directa del proveedor: limitaciones y exoneraciones. La aceptación de los servicios "tal cual están" y "según estén disponibles" ("*as is*" y "*as available*")", en este mismo capítulo.

36 En efecto, a menudo puede observarse, en la redacción contractual, cómo generalmente se asume el acuerdo de nivel de servicio comprometiéndose con el resultado, con la utilización de términos del tipo "cumpliremos con el actual ANS", "cumpliremos con el actual ANS" (del original en inglés "[We] will comply with the current SLA"), lo cual puede inducir a la consideración de estos niveles de prestación como obligaciones de resultado. (Traducción propia). Condiciones generales del software como servicio de gestión *Microsoft Dynamics CRM online* [en línea]. Disponible en: <<https://port.crm.dynamics.com/portal/static/1033/tos.htm>>. [Fecha de consulta: 18 de noviembre de 2016].

37 En relación a los niveles de medición del servicio de *Outsourcing* informático, ver APARICIO VAQUERO, Juan Pablo, *La nueva contratación...*, *op cit.*, pág. 93.

CAPÍTULO SEXTO

alcanzar estos objetivos de nivel de servicio no implica *per se* la resolución del contrato, sino que la resolución solo tendrá lugar en supuestos especialmente graves de incumplimiento, como ineficiencias reiteradas o manifiesta incapacidad del proveedor de mantener la prestación óptima del servicio.

Por nuestra parte, consideramos que estos objetivos de nivel de servicio sirven para determinar un potencial cumplimiento defectuoso del servicio. No obstante, como veremos en posteriores apartados, la falta de consecución de estos mínimos no implica, en muchas ocasiones, la cobertura total de los daños que pueda sufrir un usuario, por ejemplo, ante potenciales interrupciones del servicio. Ello es así debido la frecuente configuración de los denominados créditos de servicio o *service credits* como únicas compensaciones previstas por el proveedor para "compensar" al cliente y "penalizar" tales interrupciones del suministro, y a la aceptación por el cliente, a través del clausulado del contrato, de ciertos riesgos como elemento del propio servicio *cloud*³⁸.

Hemos mencionado anteriormente que los estándares, una vez incorporados en los contratos de computación en la nube a modo de objetivos de nivel de servicio, materializan el abstracto deber de diligencia profesional del proveedor. Ciertas instituciones desarrolladoras de estándares o auditores externos, por su parte, ofrecen certificaciones de cumplimiento de estándares, con lo cual el proveedor, a través de estas certificaciones, ofrece mayores garantías al cliente en cuanto a la consecución de los mínimos establecidos como objetivos de nivel de servicio³⁹. Aunque no es frecuente que se incluyan en los acuerdos de nivel de servicio, sino más bien en la información general del sitio web del proveedor, estas acreditaciones suelen implicar la implementación en los sistemas del proveedor de mecanismos técnicos de seguridad, protocolos de actuación y garantías respecto del tratamiento de datos personales, etc. Por otra parte, si el proveedor falsea la información sobre la adhesión

38 En realidad, los *service credits* no actuarían como una verdadera compensación o penalización, ya que, debido al escaso importe económico de estos mecanismos de resarcimiento, ni compensan de manera eficaz al cliente por los inconvenientes sufridos, ni actúan como medio de presión para obligar al proveedor al cumplimiento eficaz de los objetivos de nivel de servicio establecidos en el acuerdo contractual. Ver apartado "El cumplimiento defectuoso y la determinación de *service credits* como indemnización al cliente", en este mismo capítulo.

39 A modo de ejemplo, las certificaciones de la Asociación Española de Normalización y Certificación (AENOR) de cumplimiento del estándar ISO 27001 de seguridad de la información o del estándar ISO 22301 sobre continuidad del negocio; la certificación de la *Content Delivery and Security Association* de cumplimiento del estándar sobre seguridad, antipiratería y protección del contenido CPS, o la certificación de la *Cloud Security Alliance* sobre el cumplimiento sobre privacidad, seguridad y propiedad de los datos.

CAPÍTULO SEXTO

a estándares, estará llevando a cabo una práctica de publicidad engañosa⁴⁰.

3.- OBLIGACIONES DEL PROVEEDOR

Bajo nuestro punto de vista, la prestación satisfactoria del servicio de computación en la nube supondrá el cumplimiento, por parte del proveedor, no de una única obligación, sino de varias obligaciones inherentes a la naturaleza del servicio *cloud*.

Como se ha mencionado, las prestaciones derivadas de la computación en la nube se asemejan a las de otros contratos, como el depósito, la licencia de uso, el suministro mercantil, el *Hosting* o el *Outsourcing*⁴¹. Teniendo en cuenta sus conexiones con estas figuras jurídicas, pero también las peculiaridades propias de la relación jurídica, consideramos que el contenido de la prestación a la cual se obliga un proveedor de nube pública se podría dividir en tres acciones complementarias⁴²:

1) En primer lugar, el acceso ininterrumpido del usuario a los recursos (capacidad de almacenamiento, máquinas virtuales, software, redes, etc.), también llamado conectividad externa. Tal conectividad implicará la disponibilidad de los recursos computacionales a través de Internet, el mantenimiento de las instalaciones y la programación de los sistemas involucrados en la operativa de distribución del servicio que estén bajo control del proveedor, por ejemplo, a través del replicado de información entre diferentes centros de datos y la eficaz implementación de planes de recuperación ante desastres (*disaster recovery plan*). La conectividad externa se configurará en torno a la "multitenencia" que caracteriza los entornos *cloud* de implementación pública, permitiendo así que múltiples usuarios utilicen el servicio de manera simultánea y sin interferencias entre sus datos o su manejo de los

40 Art. 21 de la Ley 3/1991, de 10 de enero, de Competencia Desleal. "1. Se reputan desleales por engañosas, las prácticas comerciales que afirmen sin ser cierto: (...) c) Que un empresario o profesional, sus prácticas comerciales, o un bien o servicio ha sido aprobado, aceptado o autorizado por un organismo público o privado, o hacer esa afirmación sin cumplir las condiciones de la aprobación, aceptación o autorización. 2. La exhibición de un sello de confianza o de calidad o de un distintivo equivalente, sin haber obtenido la necesaria autorización, es igualmente, en todo caso, una práctica comercial desleal por engañosa."

41 Fruto de nuestro estudio, hemos llegado a la conclusión de que el contrato de computación en la nube es un contrato atípico y complejo. Ver capítulo "Objeto, naturaleza jurídica y características del contrato de computación en la nube".

42 Por sus características, los sistemas de computación en la nube que se implementan a través de nube privada, comunitaria o híbrida presentan, entre otras características, una mayor integración con la infraestructura informática que posee el cliente. Por ello, algunas de las obligaciones que en implementaciones de nube pública corresponden al proveedor, en otros modelos de implementación (privada, comunitaria o híbrida) pueden corresponder al cliente o a ambos. IP

CAPÍTULO SEXTO

recursos. La disponibilidad del servicio exigirá que los sistemas del proveedor estén configurados adecuadamente no solo para facilitar el acceso simultáneo de distintos equipos de los usuarios al servicio *cloud* (conectividad externa), sino también para responder a cada una de las peticiones de recursos manera rápida y sin errores.

2) En segundo lugar, y en conexión con la obligación anterior, la obligación de entregar recursos suministrados (capacidad de almacenamiento, máquinas virtuales, software, redes, etc.) de calidad. En el contexto *del Cloud Computing*, tal calidad correspondería a la suficiente elasticidad, a la fiabilidad del hardware y del software que los soporta y a un eficaz diseño de la interfaz que permita al cliente el aprovisionamiento bajo demanda con la mínima intervención del proveedor⁴³. Asimismo, puesto que generalmente el servicio implicará la transferencia de datos del cliente al proveedor y su almacenamiento remoto, este deberá custodiar de manera segura los contenidos procesados y migrados, manteniéndolos disponibles, íntegros y confidenciales para las personas autorizadas al acceso a esos contenidos⁴⁴. Una vez terminada la relación contractual, de la custodia de los datos del cliente (consumidor o empresario) en los sistemas de proveedor se deriva el deber de este de poner a disposición del cliente la información migrada, en un formato útil y que posibilite su uso sin que el cliente tenga que volver a introducir la información manualmente en los sistemas propios o de otro proveedor⁴⁵.

3) En tercer lugar, consideramos que el proveedor de servicios de computación en la nube tiene el deber de facilitar cierta información al cliente, preferiblemente antes de la suscripción del contrato y especialmente si quien contrata los servicios es un pequeño empresario o profesional⁴⁶. Dada la importancia

43 Por ejemplo, a través de sistemas automatizados.

44 Respecto de la seguridad de los datos, ver apartado "La calidad del servicio (II): la adopción de una política de seguridad adecuada", en este mismo capítulo.

45 Parece que algunos proveedores no se comprometen a devolver los datos al cliente cuando se extinga la relación contractual. A nuestro modo de ver, el alojamiento remoto de información genera un verdadero derecho de recuperación de lo alojado por el cliente, ya que este tiene la expectativa razonable de recuperar los contenidos que tiempo atrás confió al proveedor, independientemente de que haya tenido ocasión de realizar copias de seguridad durante el transcurso de la prestación. Ver apartado "La recuperación de los datos alojados por el cliente y su portabilidad a otro proveedor *cloud*", en el capítulo "Modificación, suspensión y extinción del contrato de computación en la nube".

46 La configuración o no del deber de información del proveedor como una obligación esencial del contrato dependerá, en gran medida, del concreto servicio contratado y del grado de impacto que pueda tener dentro de la actividad económica (profesional o empresarial) del cliente. Por ejemplo, no podrá ponderarse igual el deber de información a un cliente de red social, que el deber de información de un software como servicio de gestión integral a empresas, que aglutine toda la

CAPÍTULO SEXTO

que puede tener para el cliente empresario la adecuación del concreto servicio contratado a sus necesidades empresariales o profesionales, debe incluir aquellos aspectos relacionados con las medidas de seguridad implementadas, con la finalidad de que el cliente-empresario pueda cumplir con sus obligaciones en materia de protección de datos de carácter personal, a la vez que pueda ponderar sobre la adecuación del servicio a la criticidad de la información empresarial que maneja. Asimismo, consideramos que el cliente debe recibir información sobre la utilidad concreta del servicio suscrito, puesto que la efectiva adecuación de las características del servicio a lo publicitado genera expectativas en el cliente que motivarán su elección del proveedor con quien contratar para poder satisfacer de manera continuada sus concretas necesidades de computación. Igualmente, debe informar de los costes y cargas que le supone la suscripción del servicio, sean o no de carácter dinerario. Por último, consideramos que el proveedor deberá informar al cliente de los efectos derivados de la extinción del contrato, como el formato de recuperación de los datos, su portabilidad (es decir, la facilidad de transferirlos a otro proveedor sin necesidad de reintroducirllos manualmente), así como información sobre la técnica de borrado que se ejecutará sobre los datos remanentes en sistemas del proveedor y que garantizará la máxima reversibilidad del servicio *cloud*⁴⁷.

Aunque estas obligaciones son inherentes a la propia prestación del servicio, a veces no se reflejan contractualmente. En otras palabras, el proveedor no siempre asume compromisos relacionados con un mínimo de calidad o continuidad en la prestación del servicio o con la devolución de los datos migrados, a modo de objetivos de nivel de servicio. Ello es así porque, al ser el propio proveedor quien predispone el contrato de adhesión que deberá suscribir el cliente (consumidor o empresario) que quiera acceder al servicio, puede no incorporar un acuerdo de nivel de servicio o cláusulas que se refieran a estos extremos. En estos casos, el contrato quedará sujeto a un abstracto deber de diligencia profesional del proveedor de servicios de computación en la nube, y debiéndose tomar como referencia a tal efecto, y a falta de regulación específica, los usos del sector.

A continuación, analizaremos con más detalle las anteriores obligaciones

información que tiene la empresa sobre sus clientes, y que aloje remotamente esos datos, permita editarlos y transmitirlos en línea entre los empleados autorizados.

47 Aunque se consideran igualmente obligaciones del proveedor de servicios de *Cloud Computing*, por motivos de una mejor sistematización, las cuestiones sobre recuperación, portabilidad e información sobre el destino de los datos remanentes serán tratadas con detalle en el capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube", en este mismo trabajo.

CAPÍTULO SEXTO

contractuales, específicas del proveedor de servicios *cloud*. Posteriormente, nos referiremos a las prestaciones defectuosas y, analizaremos el contenido del deber de información del proveedor al cliente de servicios de computación en la nube.

3.1. La disponibilidad y su relación con la continuidad en la prestación

El disfrute del servicio que percibe el cliente (consumidor o pequeño empresario) depende en gran medida de la disponibilidad de los recursos computacionales que ofrece el proveedor. En efecto, dado que el servicio de nube pública se presta a través de Internet, la falta de acceso a los recursos computacionales no siempre será imputable al proveedor *cloud*, aunque este deberá asegurar que sus sistemas están plenamente operativos para exportar e importar datos en tránsito y para proporcionar los recursos informáticos que haya podido contratar cualquiera de sus clientes.

Una de las dificultades que se presentan a la hora de verificar el cumplimiento de esta obligación es la definición jurídica del concepto de disponibilidad⁴⁸. El estándar ISO/IEC 27000 define la disponibilidad como "acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran"⁴⁹. Siguiendo con esta definición, distinguiremos entre la disponibilidad de los datos y la disponibilidad del servicio de computación en la nube, ya que ambos términos integran un diferente contenido contractual.

En el primer supuesto, la disponibilidad entendida como la accesibilidad a los datos consistiría en aquella característica de los datos que garantiza el acceso ininterrumpido a su contenido por parte de las personas autorizadas (en nuestro caso, al cliente de los servicios de computación en la nube). Cuando el servicio prestado supone el acceso, a través de un dispositivo conectado a Internet, a los datos

48 A falta de un concepto jurídico adoptado por el ordenamiento legal vigente, queremos mencionar el artículo 4 del derogado Reglamento (CE) 460/2004 del Parlamento Europeo y del Consejo de 10 de marzo de 2004 por el que se crea la Agencia Europea de Seguridad de las Redes y la Información, que, en su artículo 4, definía la cualidad "disponibilidad" como "que los datos sean accesibles y los servicios estén operativos".

49 Traducción efectuada por la web española AENOR (<<http://www.iso27000.es/sgsi.html#seccion1>>) de la definición original recogida por la ISO/IEC 27000: "property of being accessible and usable upon demand by an authorized entity". [Fecha de consulta: 14 de noviembre de 2016].

CAPÍTULO SEXTO

que el propio cliente ha migrado y almacenado en servidores remotos del proveedor *cloud*, nos estaremos refiriendo a esta acepción del concepto de disponibilidad: la puesta a disposición de los datos migrados cuando el cliente autorizado pretenda acceder a ellos. Así, el cliente de servicios *cloud* que impliquen su acceso a datos u otros contenidos digitales deberá obtener, para que la prestación se considere cumplida adecuadamente, un acceso dinámico que responda en tiempo (prácticamente⁵⁰) real a su demanda, a los datos migrados sin que estos hayan sufrido modificaciones o sean accesibles por terceros no autorizados⁵¹.

Junto con la integridad y la confidencialidad, la disponibilidad integra uno de los pilares fundamentales de la seguridad de la información⁵². La cualidad de la disponibilidad de los datos migrados, por tanto, se entiende intrínseca al concepto de seguridad de la información, y, al igual que sucede con la confidencialidad e integridad, no aparecerá delimitada a modo de objetivo de nivel de servicio, puesto que se trata de características abstractas y no mensurables bajo parámetros predeterminados⁵³. Sin embargo, el proveedor está obligado a mantener la seguridad de los datos migrados como obligación principal del contrato, al formar parte de su deber de diligencia.

En el segundo supuesto, cuando nos referimos a la disponibilidad del servicio *cloud* estamos considerando otra acepción diferente del concepto de disponibilidad. Como sabemos, el objeto de los servicios *cloud* consiste, además del acceso a datos migrados por el cliente, en el suministro de recursos computacionales (aplicaciones software, capacidad de almacenamiento remoto, máquinas y redes virtuales, etc.⁵⁴). En estos casos, al hablar de disponibilidad del servicio hacemos mención, en primer

50 Teniendo en cuenta la potencial latencia de la red, es decir, el tiempo de demora que tarda Internet en transportar la información desde el sistema del proveedor hasta el dispositivo del usuario receptor. (Definición propia).

51 Por ejemplo, una empresa usuaria de un SaaS (software como servicio) de *Customer Relationship Management* o CRM (herramienta de gestión de marketing inteligente, gestión de ventas y servicio al cliente, como la solución *Microsoft Dynamics CRM*) está contratando, aparte del uso de la aplicación de gestión, el acceso a los datos de sus clientes, que previamente habrá almacenado en el sistema del proveedor cada vez que su operativa interna lo requiera. Además, se desprende de la naturaleza del contrato el requisito de que tales datos no hayan sido accedidos o modificados por terceros no autorizados por la propia empresa usuaria.

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

53 Aunque podrá comprobarse si se cumplen o no la integridad, confidencialidad y disponibilidad de los datos migrados a través de herramientas técnicas de medición del servicio prestado al cliente, su reflejo contractual se establecerá bajo la acepción genérica "seguridad de los datos", "seguridad de la información" o similares.

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

CAPÍTULO SEXTO

lugar, a la conectividad externa al servicio (es decir, a permitir que el sistema del proveedor se conecte con el equipo del cliente) y, en segundo lugar, al tiempo que tardarán los sistemas del proveedor, de acuerdo con la configuración del servicio contratado, en responder a las peticiones de recursos del cliente y proporcionar esos recursos sin errores⁵⁵. De ambas disponibilidades (del servicio y de los datos migrados) dependerá que el servicio *cloud* sea plenamente operativo y de calidad⁵⁶.

Así, en resumen, un servicio *cloud* plenamente operativo permitirá al cliente efectuar una petición de recursos al sistema *cloud* para que sea procesada con inmediatez, es decir, facilitará la conectividad externa del equipo del usuario al servicio *cloud* que ha contratado y configurará el equipo para que responda a esa petición de recursos forma rápida y sin errores. Cuando esta petición se refiera al recurso de almacenamiento, es decir, al acceso a datos migrados, la propia configuración del servicio deberá permitir tal acceso al cliente autorizado (que previamente se habrá autenticado introduciendo claves de usuario u otros mecanismos de identificación), permitiendo que los datos migrados queden disponibles para ese cliente.

En los contratos de servicios *cloud*, esta segunda acepción de disponibilidad relacionada con la operativa, es decir, la disponibilidad del servicio, es la que se presenta mayormente como objetivo de nivel de servicio (ONS). Se expresa a través de un porcentaje, conocido con el nombre de "factor de disponibilidad" (en el caso que nos ocupa, referido a un sistema *cloud*), e indica el tiempo de actividad estimado del sistema respecto del tiempo total durante el cual el sistema supuestamente debería estar operativo⁵⁷. Este porcentaje integra el principal parámetro que permite expresar el nivel de continuidad en la prestación al cual se compromete el proveedor al suscribirse el acuerdo de nivel de servicio y a mantener el suministro de recursos

55 *Conectividad externa*. "Potencial del servicio *cloud* para conectarse a sistemas externos al propio servicio (como pueden ser los dispositivos informáticos del cliente) así como a otros servicios *cloud*, o para sincronizarse con estos". Directrices de la Comisión Europea, en su documento *Cloud Service Level Agreement Standardisation Guidelines* [en línea], pág. 17. Disponible en: <<https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>>. [Fecha de consulta: 14 de noviembre de 2016].

56 Siempre y cuando hablemos de un servicio *cloud* que provea al cliente el almacenamiento de datos en los sistemas informáticos remotos del proveedor.

57 En la actualidad, esta misma definición puede extenderse a la disponibilidad de redes, aplicaciones informáticas o sistemas operativos, tal y como reconoce el informe del *Cloud Standards Customer Council* "Practical Guide to Cloud Service Agreements Version 2.0" [en línea], pág. 20. Disponible en: <http://www.cloud-council.org/CSCC_Practical_Guide_to_Cloud_Service_Agreements_Version_2.0.pdf>. [Fecha de consulta: 14 de noviembre de 2016].

CAPÍTULO SEXTO

de forma accesible desde el equipo del cliente.

A modo de ejemplo, veamos parte de un acuerdo de nivel de servicio (ANS)⁵⁸, en el cual se determina el objetivo del nivel de servicio sobre conectividad externa⁵⁹:

"Durante el periodo de vigencia del acuerdo de [el servicio], o de las versiones previas del acuerdo que regulen el uso de [el servicio], (el "acuerdo"), la interfaz web de los servicios cubiertos por [el servicio suscrito] estará en funcionamiento y a disposición del cliente por lo menos el 99,9% del tiempo de cada mes natural (el "Acuerdo de Nivel de Servicio [del servicio suscrito]"). En el caso de que [el proveedor] no cumpla el Acuerdo de Nivel de Servicio de [el servicio suscrito] y el cliente cumpla las obligaciones recogidas en este acuerdo, el cliente podrá recibir de su distribuidor los Créditos de Servicio que se indican a continuación. La resolución de este [Acuerdo de Nivel de Servicio] será el único recurso legal del cliente en caso de que [el proveedor] no ofreciera el servicio acordado".

El cálculo de este parámetro, de acuerdo con el contrato, se realiza del siguiente modo:

$$\text{Tiempo de Actividad Mensual (\%)} = \frac{\text{Total de Minutos de un determinado mes natural} - \text{Número de Minutos de Inactividad registrados durante ese mes}}{\text{Total de Minutos de un determinado mes natural}}$$

Si se incumplen las condiciones previstas en el acuerdo de nivel de servicio y dependiendo del concreto motivo que haya provocado la inactividad del servicio, el cliente empresario puede ser "compensado" (por ejemplo, mediante créditos de servicio). Para recibir una compensación por este incumplimiento del factor de disponibilidad, deberán tenerse en cuenta, además, las limitaciones y exclusiones de responsabilidad que, en su caso, haya aceptado el cliente al suscribir el contrato⁶⁰.

58 Es interesante destacar que, como regla general, únicamente los servicios *cloud* sujetos a contraprestación dineraria incorporan este tipo de compromisos sobre la continuidad del servicio en sus condiciones generales. Por lo general, los servicios prestados a cambio de otras retribuciones no dinerarias (datos personales, cesión de derechos sobre datos, visualización de anuncios publicitarios, etc.) no concretan ningún compromiso en cuanto a la disponibilidad, sino que únicamente manifiestan la voluntad del proveedor de prestar un servicio adecuado. Mediante cláusulas en las que el suscriptor acepta el uso de unos servicios "tal y como están" ("*as is*") y "según estén disponibles" ("*as available*"), se consigue una aceptación del servicio, por parte del cliente, sin mínimos de calidad o continuidad exigibles.

59 Acuerdo de nivel de servicio del SaaS (software como servicio) *Google G-Suite* [en línea], que ofrece varias aplicaciones web semejantes a las tradicionales *suites* ofimáticas (procesadores de texto, calendarios, correo electrónico, etc.). Disponible en: <<https://gsuite.google.com/intl/es/terms/sla.html>>. [Fecha de consulta: 16 de enero de 2017].

60 Ver apartado "El cumplimiento defectuoso y la determinación de *service credits* como indemnización al cliente", en este mismo capítulo.

CAPÍTULO SEXTO

3.2.- La calidad del servicio suministrado (I): el control en el aprovisionamiento de recursos y la adaptabilidad a las necesidades del cliente

El principal motivo que conduce a la pequeña empresa a contratar servicios de computación en la nube es que se le proporcionen, a través de Internet, la cantidad justa de recursos informáticos que necesita del proveedor, en atención a sus necesidades operativas y empresariales⁶¹. Independientemente del concreto tipo de servicio *cloud* contratado (infraestructura, plataforma o software como servicio), la calidad del suministro dependerá principalmente de la facilidad de la integración del servicio en la operativa empresarial del cliente y de la manera en que sus funcionalidades satisfacen las expectativas del cliente en relación a lo ofrecido por el proveedor.

Los servicios de computación en la nube pública, objeto de este trabajo, suelen comercializarse masivamente. Pero su diseño a modo de autoservicio⁶² y sus características elasticidad⁶³ y escalabilidad⁶⁴ permiten al cliente cierto grado de personalización a través de opciones en su interfaz fácilmente configurables, y de suplementos o mejoras accesorios que permitan aumentar los eventuales límites de recursos⁶⁵.

A continuación, observaremos el diferente grado de control de los recursos que puede tener un cliente *cloud* y en qué modo se refleja en la distribución de

61 La cantidad de recursos suministrados se relacionan con la elasticidad, la escalabilidad y el aprovisionamiento dinámico del servicio. Ver capítulo "Concepto y características técnicas de la computación en la nube".

62 Autoservicio bajo demanda. Característica de la computación en la nube que permite al cliente proveerse por sí mismo de capacidades de computación, a través de mecanismos automatizados y sin necesidad de intervención de cada uno de los proveedores, en el momento preciso en que los requieran. Ver capítulo "Concepto y características técnicas de la computación en la nube".

63 Elasticidad. Característica de los sistemas de computación en la nube que permite al cliente abastecerse de capacidades de computación y liberar aquellas que no se usan, de manera automatizada. Ver capítulo "Concepto y características técnicas de la computación en la nube".

64 Escalabilidad. Habilidad de un sistema o proceso para reaccionar y adaptarse rápidamente a cambios en la demanda, manejando el crecimiento continuo de trabajo de manera fluida sin perder calidad en los servicios ofrecidos. Ver capítulo "Concepto y características técnicas de la computación en la nube".

65 Por ejemplo, al contratar un software como servicio (SaaS) de alojamiento de datos, podemos configurar ciertos aspectos sobre la compartición de recursos o la edición de información. Asimismo, podemos contratar ampliaciones de la capacidad de almacenamiento virtual, por ejemplo, podemos aumentar la capacidad de un *terabyte* (1000 *gigabytes*) a varios *terabytes*, o ampliar el número de usuarios que pueden acceder al sistema *cloud* bajo la misma licencia.

CAPÍTULO SEXTO

responsabilidades entre ambas partes.

3.2.1. La infraestructura, plataforma y aplicación como productos informáticos y el grado de control de proveedor y cliente sobre ellos

Lo característico del modelo *Cloud Computing* es que configura tradicionales productos informáticos (hardware, entornos de desarrollo y software) a modo de servicio, tal y como indican las denominaciones "infraestructura como servicio" (IaaS), "plataforma como servicio" (PaaS) y "software como servicio" (SaaS)⁶⁶. Este cambio se consigue gracias a un nuevo modelo de comercialización⁶⁷ que implica un diferente grado de actividad para el proveedor en comparación con los productos informáticos tradicionales⁶⁸. Con el nuevo entorno en la nube, se suministran en formato digital (es decir, intangible), a través de banda ancha; de manera continuada (ininterrumpida) y a multitud de destinatarios simultáneamente; se prestan bajo demanda y a modo de autoservicio (el cliente es quien almacena y manipula sus datos, no el proveedor, aunque para hacerlo aquel utilice los recursos de este), de manera escalable, y en ocasiones, su contraprestación se fundamenta en el volumen de recursos consumidos⁶⁹.

66 Los servicios de computación en la nube difieren con la infraestructura o el software distribuidos de manera tradicional. Estos últimos han sido definidos por otros autores, como un "producto". Según DAVARA RODRÍGUEZ, son bienes informáticos "todos aquellos elementos que conforman el sistema en cuanto al hardware, (...) así como los elementos inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático". Por contra, entiende como servicios informáticos "todos aquellos que sirven de apoyo y complemento a la actividad informática en una relación de afinidad directa con ella". DAVARA RODRÍGUEZ, M.A, *Manual de Derecho Informático*, Pamplona, 9ª edición, 2007, pág. 262. En el mismo sentido, APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática...*, op. cit., pág. 7. Aunque, en nuestra opinión, la naturaleza del contrato de computación en la nube es un contrato de servicios, muchos proveedores no se refieren en estos términos a su prestación, sino que afirman comercializar "productos" *cloud*. Consideramos esta denominación meramente comercial, porque en realidad lo que se oferta son paquetes de servicios *cloud*, puesto que el contrato *cloud* implica otras obligaciones añadidas del proveedor (como la disponibilidad, la transmisión de los datos, la recuperación y portabilidad, etc.), que se configuran como obligaciones principales de la prestación, y de las cuales carecería si su actividad consistiera en la venta de un producto informático físico, o si de una compraventa al uso se tratase. Ver capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

67 Ver "Definición de *Cloud Computing* por el NIST", en el capítulo "Concepto y características técnicas de la computación en la nube".

68 APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática...*, op. cit., pág. 112.

69 En efecto, en ocasiones estos recursos se facturan al igual que el suministro eléctrico, por ejemplo, con servicios de almacenamiento de datos, por el espacio de memoria ocupado. En otras ocasiones, sin embargo, se contraprestan de manera similar a los bienes, de acuerdo con el número de usuarios que acceden a ellos, a través de un precio fijo por usuario.

CAPÍTULO SEXTO

En cuanto al grado de control y flexibilidad que pueda tener el cliente sobre los recursos que se le suministran a través de los entornos en la nube, este puede variar considerablemente, dependiendo del proveedor y de su concreta configuración del modelo de servicio⁷⁰. Si bien en ciertos aspectos puede resultar más o menos clara la distribución de las responsabilidades de cada parte, en otros casos podrá matizarse de acuerdo con el tipo de servicio y el margen de maniobra que pueda tener el usuario sobre los recursos proporcionados⁷¹.

El usuario puede tener el control absoluto en ciertos aspectos del servicio (por ejemplo, a través de la configuración y la activación de comandos, en relación a determinadas características de su cuenta o al procesamiento de los datos migrados)⁷²; en otros aspectos, el control puede depender exclusivamente del proveedor (por ejemplo, la cantidad de recursos que el proveedor pone a disposición del cliente de acuerdo con su suscripción); y, en otras ocasiones, dependerá de la colaboración de ambos (como sucede en el caso de responder a determinadas peticiones del cliente sobre el servicio que el proveedor deba activar o aprobar, o en ciertas configuraciones sobre seguridad de los sistemas)⁷³.

En atención a las características de cada modelo de servicio, los escenarios más habituales de distribución del control sobre los recursos entre proveedor y cliente dentro de entornos de nube pública son los siguientes⁷⁴:

1.- En modelos de servicio de infraestructura (IaaS), el control dependerá del grado de automatización de la máquina virtual suministrada. Habitualmente, el

70 Mediante los tradicionales contratos de *outsourcing*, los clientes controlan el servicio a través de las estipulaciones contractuales y de las instrucciones a los proveedores (entendiendo el control como el dominio necesario del servicio para conseguir que se adapte a sus necesidades empresariales. El cliente de nube pública tendrá siempre de un control inferior al que le correspondería si contratase un sistema de *Outsourcing*, similar al modelo de nube privada. Ver el apartado dedicado al *Outsourcing* en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

71 Por ejemplo, en casos de problemas derivados de la infraestructura física y virtual que soporta el servicio, el cliente posiblemente quede exento de responsabilidad, puesto que en ocasiones quien posee el control sobre el adecuado funcionamiento de infraestructura es únicamente el proveedor (o subproveedores, en su caso). Sin embargo, en algunos servicios de infraestructura, el cliente puede tener el control sobre la configuración de ciertos aspectos de la máquina virtual que le ha sido suministrada por el proveedor.

72 Un ejemplo práctico podría ser cómo se configura la compartición de información migrada con terceros elegidos por el usuario.

73 KUAN HON, W; MILLARD, C, "Control, Security, and Risk in the Cloud", *Cloud Computing Law*, (Coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 27.

74 KUAN HON, W; MILLARD, C, *Control, Security..., op. cit.*, pág. 28. Ver asimismo Figura 2, en el capítulo "Concepto y características técnicas de la computación en la nube", de los mismos autores.

CAPÍTULO SEXTO

cliente ostenta un mayor control y flexibilidad sobre la administración y configuración de diferentes componentes respecto a servicios de plataforma o software, y puede ajustar, hasta cierto punto, la respuesta de la máquina virtual a los comandos que permiten el procesamiento de los datos y que el propio cliente introduce en esa máquina virtual. Así, el cliente tiene margen de maniobra para configurar el sistema operativo de la máquina virtual, establecer comportamientos predeterminados o conexiones con otras máquinas o redes virtuales, ejecutar aplicaciones en ella, instalar software de seguridad adicional al facilitado por el proveedor, etc. La necesidad de una mayor capacidad de gobierno en materia de seguridad y funcionalidad de los recursos supone uno de los principales alicientes para contratar modelos de infraestructura como servicio, junto con la obtención de mayor capacidad de procesamiento o almacenamiento.

2.- En modelos de plataforma como servicio o PaaS, el proveedor suele tener mayor control sobre la red y el almacenamiento remoto de los datos que en modelos *cloud* de software como servicio. En los PaaS, el cliente generalmente puede configurar aspectos relacionados con la interfaz, el software que conecta ordenadores y dispositivos con aplicaciones (también llamado *middleware*)⁷⁵, el software que conecta aplicaciones entre sí (las denominadas APIs)⁷⁶, y otras herramientas de desarrollo de aplicaciones.

3.- En modelos de software como servicio o SaaS, el cliente prácticamente no tiene capacidad de maniobra en cuanto a la seguridad de los datos o de la aplicación, sino que únicamente aprovechará las funcionalidades predeterminadas que le ofrece esa aplicación y, en su caso, migrará sus datos a sistemas del proveedor. Ello no impide que el diseño de la aplicación permita la configuración de unos aspectos mínimos, por ejemplo, relacionados con aspectos de búsqueda de información, compartición de archivos con terceros, opciones de privacidad, etc.

75 El llamado *middleware* es una plataforma que se sitúa entre el sistema operativo y la aplicación informática, y ayuda a funcionalidades como la integración de tareas simultáneas, mensajería, etc. JANSEN, Dale; JANSEN, Cory, "What Clouds Middleware mean?", *Technopedia, the IT Education Site* [en línea]. Disponible en: <<https://www.techopedia.com/definition/30630/cloud-middleware-software>>. [Fecha de consulta: 23 de noviembre de 2016].

76 La *Application Programming Interface* es un software que permite la interacción entre diferentes componentes lógicos de programas informáticos. Las APIs posibilitan a los programadores el diseño de aplicaciones que no interrumpen su funcionamiento aunque el software que las sustenta vaya actualizándose continuamente. JANSEN, Dale; JANSEN, Cory, "What does Application Programming Interface mean?", *Technopedia, the IT Education Site* [en línea]. Disponible en: <<https://www.techopedia.com/definition/24407/application-programming-interface-api>>. [Fecha de consulta: 23 de noviembre de 2016].

CAPÍTULO SEXTO

Dicho lo anterior, el proveedor de computación en la nube pública, sea cual sea el modelo o modelos de servicio que presta (infraestructura, plataforma o software como servicio), siempre posee el control sobre los equipos físicos, siendo una de sus obligaciones principales su adquisición, actualización y mantenimiento, así como el aislamiento de los datos migrados por diferentes clientes que comparten el mismo contenedor de recursos⁷⁷. Por otra parte, el cliente puede mejorar la seguridad del servicio con diferentes precauciones y la adopción de sus propias medidas de seguridad, complementarias a las proporcionadas por el proveedor. Por ejemplo, puede realizar sus propias copias de seguridad adicionales, instalar aplicaciones que permitan el encriptado o fragmentado de datos, proteger de terceros sus credenciales de acceso, etc.

De lo anterior se extraen dos conclusiones. La primera, que el cliente de nube pública poseerá un mayor control y responsabilidad por los datos en los servicios de infraestructura, que irá decreciendo en los servicios de plataforma, y que será aún menor en los servicios de software⁷⁸. La segunda conclusión, como han advertido ya algunos autores, es que esta diferente distribución del control puede verse reflejada a la hora de verificar ciertas obligaciones y responsabilidades derivadas de los concretos recursos, especialmente en cuestiones relacionadas con la seguridad o efectos sobre el correcto funcionamiento del servicio para el cliente o para otros usuarios, con lo cual puede resultar relevante a la hora de delimitar el deber de diligencia de cada parte contractual⁷⁹.

Bajo nuestro punto de vista, no resulta práctico realizar una clasificación general sobre qué aspectos de cada servicio corresponderá a una u otra parte tener bajo control, puesto que la configuración del servicio y del contrato pueden desvirtuar las presunciones generales. Lo especialmente relevante es atender a la regulación en las condiciones generales de las responsabilidades entre las partes, de acuerdo con el específico servicio contratado por el pequeño empresario y al efectivo grado de control que cada una de ellas pueda tener respecto de los riesgos de la prestación. Por último, debemos tener en consideración la eventual existencia de subcontrataciones a las cuales haya podido recurrir el proveedor para poder proporcionar el servicio al cliente final y a la validez de potenciales exclusiones y

77 Recordemos, no obstante, que el proveedor que presta su servicio al cliente final puede tener subcontratado a otro proveedor que gestione el centro de procesamiento de datos físico.

78 WINKLER, Vic; "Data Security in Cloud Computing. Part 1. Overview" [en línea], *EETimes*, 2011. Disponible en: <http://www.eetimes.com/document.asp?doc_id=1278914&print=yes>. [Fecha de consulta: 18 de mayo de 2017].

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

CAPÍTULO SEXTO

limitaciones de responsabilidad que pueda efectuar el proveedor en caso de que se produzca algún incidente durante la prestación, para determinar quién deberá, finalmente, asumir sus consecuencias jurídicas.

A continuación veremos el papel que juegan las necesidades computacionales del cliente y su satisfacción por el proveedor en el ámbito de la responsabilidad contractual.

3.2.2. La responsabilidad del proveedor por la adaptabilidad del servicio a las necesidades del cliente y su relación con el deber de información precontractual

Si bien al proveedor *cloud* que contrate con consumidores le es exigible el deber de información precontractual sobre las concretas prestaciones que ofrece el servicio y sobre la funcionalidad de los contenidos digitales que se suministrarán (entre otros extremos), de acuerdo con el art. 97 del TRLGDCU, nada dice la normativa sobre que estas obligaciones se mantengan cuando el suscriptor sea un pequeño empresario⁸⁰.

Sin embargo, puesto que la naturaleza técnica del servicio de computación en la nube puede resultar compleja para el pequeño empresario suscriptor, y de acuerdo con la buena fe contractual y el deber de diligencia del proveedor, consideramos que esta información debería ser facilitada igualmente a aquel pequeño empresario que pretenda suscribir servicios de computación en la nube, especialmente antes de que se proceda a su contratación, para que pueda valorar si el servicio se adapta o no a lo que requiere su actividad empresarial⁸¹.

80 Al respecto de las exigencias de la información precontractual en contratos de servicios de computación en la nube, cabe mencionar los trabajos del Grupo de Expertos en contratos de computación en la nube de la *Cloud Computing Strategy*. Por una parte, en sus documentos preparatorios sugieren una determinada información que debería aportarse en el marco de la contratación de la computación en la nube (concretamente: nociones sobre qué es y cómo funciona la nube, qué servicios ofrece el proveedor, si son servicios a través de nube pública, híbrida o privada, qué términos contractuales se le aplican al suscriptor, cuánto y cómo debe pagar por el servicio, cómo funciona el sistema de copias de seguridad, que límites de capacidad tiene el servicio, etc.) . Por otra, las diferentes expectativas de información del suscriptor consumidor y del suscriptor pequeño empresario. A este último le interesa conocer información sobre la localización de los datos, las garantías sobre su confidencialidad, y cómo se asegura su recuperación. También se pone de manifiesto que la necesidad de transparencia debe mantenerse durante toda la cadena de subcontrataciones. EU CLOUD COMPUTING EXPERT GROUP, *Discussion paper on pre-contractual information* [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 18 de mayo de 2017].

81 Dice CORRIPIO: "En situaciones de desequilibrio subjetivo o actuando en el marco de las relaciones profesional-profano, deviene necesario tutelar la confianza legítima que una parte deposita en la otra durante los tratos y corregir el desequilibrio subjetivo". CORRIPIO GIL-DELGADO, M^a Reyes, *El deber de*

CAPÍTULO SEXTO

El deber de información precontractual en los contratos informáticos puede dividirse, según afirma la doctrina, en diferentes obligaciones. Estas obligaciones, en nuestra opinión, son predicables de los contratos de *Cloud Computing*⁸². La primera de ellas consiste en facilitar información técnica sobre el funcionamiento y prestaciones del servicio. Ello se podría traducir, en el contexto de la nube, en la descripción clara sobre qué ofrece el proveedor: la virtualización de infraestructura y su potencia, entornos de desarrollo y herramientas incluidas, uso de aplicaciones informáticas y sus funcionalidades, eventuales límites de accesos al servicio (máximo número de usuarios contratado, etc.) o de las capacidades prestadas (máxima capacidad de almacenamiento), mejoras de la implementación del servicio en el rendimiento informático de la empresa, etc. En caso de que las actividades incluidas en las prestaciones del proveedor no queden suficientemente delimitadas, podrán interpretarse o deducirse en atención a los deberes del proveedor de diligencia, colaboración y buena fe, a la información facilitada en fase precontractual y a los usos de la industria⁸³.

La segunda obligación consistiría en prestar consejo y resolver las dudas del cliente. Este deber de consejo comprende, según la doctrina, diferentes deberes para el proveedor, tales como recabar información del cliente sobre sus necesidades para poder aconsejarle con conocimiento de causa; suministrar información objetiva y exacta sobre las posibilidades de la solución informática propuesta y advertir al cliente sobre sus características y aplicaciones; aconsejarle y proponer el producto o solución que mejor se adapte a sus necesidades; e informarle de los riesgos que entraña la adquisición de ese producto o servicio informático (dificultades técnicas, incompatibilidades, etc.)⁸⁴.

Si bien consideramos exigibles las obligaciones anteriores para el proveedor, pensamos que este no queda obligado a prestar un servicio específicamente adaptado a las concretas necesidades concretas de cada cliente suscriptor. Al tratarse de servicios comercializados en masa, el proveedor de nube pública no personaliza el producto para el cliente, a diferencia de lo que sucede en los modelos de implementación de nube privada o comunitaria o en el *Outsourcing*, sino que el servicio se ofrece de manera estandarizada para que los clientes interesados puedan

información precontractual, Madrid, 1999, pág. 279.

82 CORRIPIO GIL-DELGADO, M^a Reyes, *El deber de...*, op. cit., págs. 281 y ss.

83 APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática. Introducción al outsourcing de los sistemas de información*, 1^a edición, Granada, 2002, pág. 92.

84 CORRIPIO GIL-DELGADO, M^a Reyes, *El deber de...*, op. cit., págs. 282, 289.

CAPÍTULO SEXTO

proceder a su contratación. Forma parte del deber de diligencia profesional del pequeño empresario, tras una eficaz labor de comparación entre los diferentes proveedores de servicios similares, la selección del servicio que se le presente como más adecuado y con mayores garantías. Lo anterior no obsta, sin embargo, a que el proveedor se vea obligado a prestar el servicio conforme a las informaciones facilitadas precontractualmente (art. 1258 Código Civil).

Por otro lado, el diseño del servicio resulta relevante en cuanto a la satisfacción de las necesidades del cliente. La flexibilidad de control del suministro de la que disponga el cliente le permitirá atender a la demanda de recursos informáticos que presente en cada momento (lo cual supone una de las ventajas que ofrece la computación en la nube: la elasticidad de los recursos). Del mismo modo, el diseño del servicio también determinará, como hemos visto en el anterior apartado, qué aspectos del servicio puede gestionar el cliente y qué aspectos dependen de la actuación del proveedor, con lo cual podrá escoger el servicio que le permita el control más ágil y eficiente de los recursos de acuerdo con las concretas demandas que presente su operativa empresarial.

La naturaleza de la obligación de proporcionar un servicio de calidad de acuerdo con lo ofertado se configura, a nuestro parecer, como una obligación que no obliga al proveedor a supervisar la efectiva adaptación a las necesidades del cliente y a personalizar el servicio como sucedería con el *outsourcing*⁸⁵ (puesto que estamos hablando de servicios comercializados en masa y de contratos no negociados)⁸⁶, aunque sí sería responsable de informar sobre los usos y funcionalidades del servicio de manera clara y previa a la contratación, de que el servicio responda realmente a tales especificaciones establecidas, y a responder a las consultas que el cliente pueda realizar para asegurar que se cubren sus expectativas⁸⁷. Además de lo anterior, debe

85 APARICIO VAQUERO, Juan Pablo, *La nueva contratación...*, *op. cit.*, págs. 60, 113.

86 En otros contratos, se recoge de forma expresa esta exclusión, equivalente a aceptación de los servicios "tal cual están". Por ejemplo, el contrato de SaaS (Software como Servicio) *Google Apps* para empresas afirma: "en la medida en que la ley lo permita, a menos que quede expresado de otro modo en este documento, ninguna de las partes ofrece ninguna otra garantía de ningún tipo, implícita ni explícita, obligatoria, estatutaria ni de otra clase incluidas, sin limitarse a ello, las garantías de comerciabilidad, adecuación para un fin particular, (...)".

87 Consideramos, en este aspecto, aplicable analógicamente, la afirmación que realiza APARICIO en relación a la necesidad, en la obligación de desarrollo de programas informáticos, de que lo que interesa al cliente es la consecución de este resultado, con independencia de los medios y diligencia empleados. Por ejemplo, al cliente le importará que el SaaS (Software como Servicio) de gestión de gestión de datos de clientes o CRM realmente prestado coincida con las funcionalidades, especificaciones y compatibilidades publicitadas por el proveedor, independientemente de los medios empleados por los creadores de la aplicación informática. Del

CAPÍTULO SEXTO

tenerse en cuenta que contractualmente el proveedor suele eximirse de cualesquiera responsabilidades por daños derivadas de una falta de adecuación del servicio a la actividad del cliente⁸⁸.

Resumiendo lo dicho en anteriores apartados, en nuestra opinión son exigibles al proveedor tres extremos en relación a la calidad del suministro de los recursos del servicio como obligación principal del contrato *cloud*: el primero, la elasticidad de los recursos (hasta el límite contratado, si lo hubiera); el segundo, la adecuación a lo publicitado al cliente en la oferta contractual en relación a las funcionalidades del recurso o recursos a suministrar (infraestructura, plataforma, software o una combinación de estos); y por último, el adecuado diseño y mantenimiento, por una parte, de los equipos físicos que sustentan el entorno de la nube, y por otra, de los elementos de software que permiten al cliente su uso útil y eficiente (interfaz, sistemas operativos, herramientas de autoconfiguración, etc.). El cumplimiento de estas obligaciones está íntimamente relacionado con el deber de información (pre y post-contractual⁸⁹) del proveedor y con el deber de colaboración del cliente (pequeño empresario o profesional) con este, siendo esencial para el éxito de la relación jurídica la transparencia entre ambas partes⁹⁰. Asimismo, consideramos que al proveedor no le es exigible la completa adaptabilidad de un servicio comercializado en masa a las necesidades concretas de cada cliente, pero sí el acceso continuado en línea a los recursos (característico de la prestación del servicio *cloud*⁹¹) y la adecuación de este servicio a las características promocionadas, puesto que crean expectativas legítimas en el cliente que propician la contratación de un concreto servicio con un determinado proveedor.

mismo modo, la infraestructura o la plataforma suministrada en los servicios IaaS o PaaS debe adecuarse a las especificaciones y características técnicas que crean expectativas en el cliente, y quien espera ese concreto resultado cuando contrata. APARICIO VAQUERO, Juan Pablo, *La nueva contratación...*, *op. cit.*, pág. 112.

88 Ver apartado "Responsabilidad directa del proveedor: limitaciones y exoneraciones. (...)", en este mismo capítulo.

89 Es posible que, en el transcurso de la relación contractual, el proveedor vaya mejorando y actualizando la seguridad de sus sistemas debido a necesidades técnicas de la industria, con lo cual pueden producirse cambios entre las especificaciones sobre seguridad facilitadas al cliente en la fase precontractual y futuras adaptaciones de equipos y protocolos de seguridad.

90 En relación al deber de colaboración del cliente empresario, si tiene dudas sobre la utilidad o seguridad de las funcionalidades y capacidades de computación de las cuales pretende que le abastezca el proveedor, es recomendable que, en virtud de su deber de diligencia profesional, intente recabar del proveedor la máxima información posible.

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

CAPÍTULO SEXTO

3.3.-La calidad del servicio (II): la adopción de una política de seguridad adecuada

En el anterior apartado hemos estudiado las obligaciones del proveedor de proporcionar el suministro de recursos adecuados en relación a las expectativas generadas en el cliente. En este apartado nos plantearemos cuál es el origen y la naturaleza de la obligación relativa a la implementación de medidas de seguridad, nos aproximaremos a la regulación contractual de las medidas de seguridad adoptadas por el proveedor con la finalidad de salvaguardar los contenidos de los usuarios y la seguridad de sus propios sistemas, y cuál será la resultante distribución de responsabilidades ante problemas relacionados con la integridad y confidencialidad de los datos digitales⁹².

3.3.1. La preservación de la integridad de los datos

La seguridad de los datos se fundamenta en tres pilares: la integridad, la confidencialidad y la disponibilidad, como hemos mencionado en apartados anteriores. Este apartado se centrará en la obligación del proveedor de servicios de computación en la nube de preservar la integridad de los datos de sus clientes, los cuales custodia en sus sistemas durante la prestación del servicio⁹³.

Tras el examen de modelos de contratos de computación en la nube que hemos realizado para el desarrollo de este trabajo de investigación, hemos comprobado que en ninguno de los contratos de servicios de infraestructura como servicio (IaaS), plataforma como servicio (PaaS) ni software como servicio (SaaS) examinados aparece definido el concepto de integridad de los datos.

La delimitación de este concepto resulta una cuestión básica en la tarea de determinar las situaciones que eventualmente generen responsabilidades. La Unión Europea definió el término "integridad de los datos" en el artículo 4 del derogado Reglamento 460/2004 de creación de la Agencia Europea de Seguridad de la Redes y la Información (ENISA), entendiéndola como "la confirmación de que los datos que se han enviado, recibido o almacenado están completos y no se han modificado"⁹⁴.

92 Se tratarán en posteriores apartados las cuestiones relacionadas con la confidencialidad y con la preservación y destino de los datos una vez terminada la relación contractual.

93 Ver apartado "Riesgos de la implementación del *Cloud Computing* por parte de las empresas", en el capítulo "Concepto y características técnicas de la computación en la nube".

94 El Reglamento 460/2004 de creación de la Agencia Europea de Seguridad de la Redes y la Información (ENISA) se derogó a través del Reglamento 526/2013, y este carece en su articulado, de la definición del concepto de integridad. Tampoco aparece definición alguna de este concepto en la Directiva marco 2002/21/CE Del Parlamento Europeo y del Consejo, de 7 de marzo de 2002,

CAPÍTULO SEXTO

Por nuestra parte, anteriormente la hemos definido⁹⁵ como aquella propiedad de los datos que garantiza su precisión, corrección y completitud durante todo el ciclo de procesamiento de la información⁹⁶. En el contexto de sistemas basados en arquitectura *cloud*, consideramos íntegros aquellos datos que no han sido destruidos, alterados o modificados de forma accidental o por personal no autorizado desde que se migran a la nube o se crean en ella hasta que finaliza la obligación contractual del proveedor de preservarlos en sus sistemas.

El proveedor suele incorporar un adecuado sistema de gestión de la seguridad de la información, y generalmente instaura mecanismos y procesos destinados a evitar la destrucción, la pérdida o la modificación no autorizada de todos o parte de los contenidos almacenados por el cliente en la infraestructura *cloud*, con el fin de preservar la característica de la integridad en los datos del cliente, y en cumplimiento de su deber de diligencia profesional⁹⁷. Son muchos los proveedores que se comprometen a adoptar medidas técnicas y organizativas mínimas, las cuales corresponderán a estándares de la industria, aunque en pocas ocasiones se especifican en las condiciones contractuales cuáles son los estándares adoptados como referencia⁹⁸. Ello no significa que el proveedor nunca facilite esa información, sino

relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.

95 (Definición propia). Ver apartado "Riesgos de la implementación del *Cloud Computing* por parte de las empresas", en el capítulo "Concepto y características técnicas de la computación en la nube".

96 Ciclo de procesamiento. Conjunto de procesos computacionales que tienen lugar desde que la información se crea dentro del sistema informático hasta que desaparece totalmente del mismo. Estos procesos comprenden copias de seguridad, tratamiento de datos de carácter personal, recuperación de datos en caso de desastre, replicado automático, y demás operaciones necesarias para administrar una estructura de almacenamiento de datos procesados digitalmente. (Definición propia).

97 El sistema de gestión de la seguridad de la información o SGSI (en inglés, *Information Security Management System* o *ISMS*) es un proceso sistemático, documentado y conocido por toda la organización para garantizar que la seguridad de la información es gestionada correctamente. (Definición extractada y traducida de la web de información sobre la norma ISO 27000). Existen diferentes modelos de SGSI. Uno de ellos es el propuesto por la norma ISO 27002:2013, que consiste en la implementación de una serie de documentos (manual de seguridad, procedimientos, instrucciones y registros) mediante un ciclo de cuatro fases: PDCA (*Plan-Do-Check-Act* o planificar, hacer, verificar y actuar). Para más información, ver el documento sobre la norma [en línea]. Disponible en: <http://www.iso27000.es/download/doc_sgsi_all.pdf>. [Fecha de consulta: 3 de agosto de 2016].

98 Las condiciones generales del software como servicio (SaaS) *Dropbox para empresas* establecen que "Dropbox utilizará, como mínimo, las medidas de seguridad técnicas y organizativas estándar del sector para transferir, almacenar y procesar los datos del cliente. Estas medidas están diseñadas para proteger la integridad de los datos del cliente y salvaguardarlos contra cualquier acceso, uso o procesamiento no autorizado de los datos del cliente". Condiciones de Dropbox para empresas [en línea]. Disponibles en: <https://www.dropbox.com/es_ES/privacy#business_agreement>. [Fecha de consulta: 27 de

CAPÍTULO SEXTO

que a menudo formará parte de otros textos que no son cláusulas contractuales, pero que, al ser publicitados en el sitio web del proveedor, pueden considerarse información precontractual y, por tanto, tener igualmente un carácter vinculante para el proveedor, a modo de mínimos a adoptar.

En nuestra opinión, aunque la obligación de adoptar unas mínimas medidas de seguridad para proteger los datos alojados en los sistemas *cloud* no se refleje en el contrato, forma parte del deber de diligencia del proveedor, porque esta condición es intrínseca a las expectativas legítimas del cliente en relación a la naturaleza del contrato⁹⁹.

A nuestro modo de ver, se plantea la cuestión jurídica de la duración del deber de diligencia del proveedor en cuanto al mantenimiento de la integridad de los datos de sus clientes que almacena en sus sistemas. Creemos que la preservación de la integridad de los datos debería alcanzar el momento en el cual los datos se devuelven al cliente una vez extinguida la relación contractual, o se transmiten a otro proveedor, puesto que hasta ese momento persiste en el proveedor el deber de diligencia como prestador del servicio *cloud* contratado, y a su vez se genera en el cliente una expectativa legítima de recuperar los datos que ha alojado en los sistemas remotos de aquel.

Por su parte, el deber de diligencia profesional del pequeño empresario exigirá una previa valoración de las ventajas y riesgos en materia de integridad antes contratar y migrar sus datos a los sistemas de un proveedor de servicios de computación en la nube. Como hemos observado, existen similitudes entre el contrato de *Cloud Computing* que implique el almacenamiento de datos del cliente en la infraestructura del proveedor¹⁰⁰ y la figura jurídica del depósito, similitudes que

diciembre de 2016].

99 En el *Outsourcing* informático tradicional, generalmente el cliente puede visitar las instalaciones en las cuales tendrá el tratamiento de los datos empresariales y se ofrece información detallada sobre los procesos técnicos y organizativos. Sin embargo, esta posibilidad no tiene lugar cuando se contratan servicios de nube pública, puesto que los datos del cliente estarán dispersos (replicados o fragmentados) en ubicaciones geográficas distintas y compartirán infraestructura con los datos de otros muchos clientes. Por tanto, el cliente *cloud* pequeño empresario deberá conformarse con revisar la información sobre la adopción de políticas de seguridad que le facilite el proveedor sobre el servicio contratado, y confiar en su cumplimiento. MARCHINI, Renzo; *Cloud Computing: a practical introduction to the legal issues*, 1ª edición, Londres, 2010, pág. 24.

100 A mayor abundamiento, queremos mencionar que el contrato de alojamiento de datos fue recogido como una nueva forma de contrato mercantil en el artículo 532-12 del Anteproyecto de Ley del Nuevo Código Mercantil (fecha del texto de la Comisión de Codificación: 17 de junio de 2013): "por el contrato de alojamiento de datos 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

CAPÍTULO SEXTO

en ocasiones podrían servir para adoptar al depósito como figura jurídica de referencia en relación al deber de custodia de los contenidos del cliente¹⁰¹.

Así, como hemos comentado, la suscripción del servicio implica que el cliente cede gran parte del control sobre la seguridad de los datos al proveedor. Sin embargo, tengamos en cuenta que el cumplimiento de este deber de diligencia puede no estar sujeto exclusivamente a la voluntad del proveedor, sino que depende, a su vez, de circunstancias externas a su control, debido a la propia complejidad de los entornos en la nube y al diseño del propio servicio *cloud*¹⁰². En los casos en que las medidas mínimas de seguridad instauradas por el proveedor no hayan sido suficientes para proteger la integridad de los datos del cliente (por ejemplo, ante ataques maliciosos o virus informáticos, fallos de hardware o software, problemas de seguridad de las telecomunicaciones o las redes, interrupciones en el suministro de energía, etc.), deberá analizarse la previsibilidad y la evitabilidad de la contingencia¹⁰³, atendiendo a las posibilidades técnicas y económicas del proveedor, con el fin de determinar si existe culpa o negligencia de acuerdo con los artículos 1104 y 1105 del Código Civil¹⁰⁴. Si la alteración en la integridad de los datos se debe a fuerza mayor en

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". Observemos que este artículo excluye los contratos gratuitos. También recoge el Anteproyecto que "el prestador de alojamiento de datos estará obligado a conservar los datos o la información alojados por el cliente y mantener su integridad", en su artículo 532-13.3.

101 El artículo 1758 del Código Civil establece que "se constituye el depósito desde que uno recibe la cosa ajena con la obligación de guardarla y de restituirla". El problema en cuanto a la asimilación de ambas figuras aparece en el artículo 1761, en el que se excluye la información como posible objeto del contrato de depósito, al afirmar que "solo pueden ser objeto del depósito las cosas muebles". Con la información en la nube sucede que el control sobre la integridad de aquello depositado es compartido, porque el usuario tiene acceso también a los datos custodiados por el proveedor. La misma cuestión se plantea en el concepto recogido por el Anteproyecto de Código Mercantil, en su art. 552, al hablar de "cosa" y no de "bien" (en cuyo caso podría aceptarse la inclusión de bienes inmateriales en el concepto): "por el contrato de depósito se obliga, a cambio de un precio, a custodiar las cosas que le entregue el depositante y a devolvérselas". Ver capítulo "Objeto, naturaleza jurídica y características de los contratos de computación en la nube".

102 Existe un diferente grado de control del cliente sobre la seguridad que deriva del propio diseño del servicio, dependiendo de si aquello contratado es un servicio *cloud* de infraestructura, plataforma o software, pueden verse afectados aspectos relacionados con la seguridad de cada uno de los componentes que integran la prestación. Asimismo, el proveedor puede tener subcontratados con terceros aspectos relacionados con la infraestructura que soporta el servicio prestado. Ver capítulo "Concepto y características técnicas de la computación en la nube".

103 DIEZ-PICAZO, Luís, *Derecho de daños*, Madrid, 1999, pág. 361.

104 Art. 1104 del Código Civil. "La culpa o negligencia del deudor consiste en la omisión de aquella diligencia que exija la naturaleza de la obligación y corresponda a las circunstancias de las personas, del tiempo y del lugar. Cuando la obligación no exprese la diligencia que ha de prestarse en su cumplimiento, se

CAPÍTULO SEXTO

atención a los arts. 1101 y 1105 del Código Civil, el proveedor o subproveedores quedarán exentos de responsabilidad porque la situación escapa de su control razonable¹⁰⁵.

A nuestro parecer, la responsabilidad que asuma el proveedor tiene que ser proporcional a la contraprestación del cliente, sin que puedan equipararse las exigencias de un contrato de pago a las de un contrato sin contraprestación dineraria, puesto que el primero debería implicar un mayor compromiso por parte del proveedor que el segundo. A pesar de lo anterior, no se puede obviar la cobertura de expectativas mínimas que el cliente legítimamente espera al suscribir un contrato que implique alojamiento remoto o procesamiento remoto de datos, derivadas de la naturaleza jurídica de tal contrato, aunque ese contrato no se remunere monetariamente¹⁰⁶.

Cuando del transcurso de operaciones que formen parte del servicio y que se presten por parte de subproveedores *cloud* se deriven alteraciones en la integridad de los datos del cliente, el proveedor principal responderá por reclamaciones ante el cliente, en virtud del artículo 1903 del Código Civil; posteriormente, el proveedor podrá ejercitar su derecho de repetición de acuerdo con el artículo 1904 del Código Civil¹⁰⁷.

Además de lo anterior, consideramos que, en aquel caso en que el subproveedor no haya instaurado en sus sistemas las medidas de seguridad mínimas que garanticen al proveedor principal la prestación del servicio en las condiciones que oferta al cliente o usuario final, puede existir culpa *in eligendo* del proveedor al seleccionar al subproveedor, teniendo en cuenta la habitual mediación de un

exigirá la que correspondería a un buen padre de familia". Art. 1105 del Código Civil. "Fuera de los casos expresamente mencionados en la ley, y de los en que así lo declare la obligación, nadie responderá de aquellos sucesos que no hubieran podido preverse, o que, previstos, fueran inevitables".

105 Sería el caso de catástrofes naturales, problemas con la red global de Internet, guerra, terrorismo, huelgas, intervenciones gubernamentales, etc.

106 Ello no implica que estemos ante un contrato no oneroso, sino que las contraprestaciones son de carácter distinto. Ver apartado dedicado a la onerosidad como característica del contrato de servicios *cloud*, en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

107 Art. 1903 del Código Civil. "La obligación que impone el artículo anterior es exigible, no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder. (...). Lo son igualmente [responsables] los dueños o directores de un establecimiento o empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones. (...) a responsabilidad de que trata este artículo cesará cuando las personas en él mencionadas prueben que emplearon toda la diligencia de un buen padre de familia para prevenir el daño". Art. 1904 del Código Civil. "El que paga el daño causado por sus dependientes puede repetir de éstos lo que hubiese satisfecho".

CAPÍTULO SEXTO

acuerdo de nivel de servicio (ANS) entre ambos, en el que subproveedor fija parámetros como garantía de la calidad de la prestación al proveedor¹⁰⁸.

Es común que los contratos incluyan cláusulas de exención de responsabilidades por cualquier circunstancia que provoque la alteración o pérdida de datos. Como veremos en posteriores apartados, es discutible que algunas de estas cláusulas tengan validez bajo el ordenamiento jurídico español, atendiendo a la naturaleza del concreto servicio *cloud* contratado y a las legítimas expectativas que se generan en el cliente¹⁰⁹.

Por su parte, tanto el administrador de las cuentas de la empresa cliente como el usuario final deben responsabilizarse por la custodia de sus claves de acceso, porque este deber de custodia que se ha delegado en aquellos escapa del ámbito de control del proveedor *cloud*, y, consecuentemente, no se le podrá exigir responsabilidad cuando por tal motivo se produzcan alteraciones o modificaciones de datos no deseadas. Esta exoneración de responsabilidad del proveedor también se incluye, como es de esperar, en muchas condiciones contractuales¹¹⁰.

A tenor de lo expuesto, sería poco realista considerar la seguridad de los datos, y en concreto la preservación de su integridad, como una obligación absoluta para el

108 Por contra, la culpa *in vigilando* entraría en juego únicamente en aquellas situaciones en las que el proveedor tiene ocasión de controlar o supervisar la seguridad de sus subproveedores. Es habitual, en aquellos casos en los que el subproveedor es una gran empresa multinacional, que no se permita conocer ciertos aspectos de seguridad a los profesionales que contratan sus servicios como soporte para sus propios sistemas de computación remota, especialmente si estos carecen de un fuerte poder de negociación, como es el caso del cliente pequeño empresario o profesional.

109 Como ejemplo, esta cláusula del software como servicio (SaaS) de almacenamiento remoto de datos del proveedor Box: "Box se esforzará al máximo en prestar los Servicios, pero Box no garantiza ni promete que el contenido que almacene o al que acceda a través de los Servicios no estará sujeto a daños involuntarios, no disponibilidad temporal, corrupción o pérdida. En la medida que lo permita la ley y salvo lo establecido en estas condiciones, Box no será responsable en modo alguno en el caso de que el contenido sea eliminado, corregido o destruido, resulte dañado, se pierda, no se almacene o no se cifre". Términos contractuales de Box [en línea]. Disponibles en: <<https://www.box.com/es-419/legal/termsofservice>>. [Fecha de consulta: 18 de mayo de 2017].

110 Dicen las condiciones del servicio *Dropbox para empresas*: "El cliente podrá designar a usuarios finales como "administradores" a través de la consola de administración. Los administradores tendrán la posibilidad de acceder, revelar, restringir o eliminar los datos del cliente de las cuentas de los servicios. Los administradores también podrán supervisar, restringir o cancelar el acceso a las cuentas de los servicios. Las responsabilidades de Dropbox no se extienden a la gestión o administración interna de los servicios. El cliente será responsable de: (i) proteger la confidencialidad de las contraseñas y las cuentas de los administradores; (ii) gestionar el acceso a las cuentas de los administradores; y (iii) garantizar que el uso de los servicios por parte de los Administradores cumpla lo establecido en este acuerdo". Términos contractuales de Dropbox para empresas [en línea]. Disponibles en: <https://www.dropbox.com/es_ES/privacy#business_agreement>. [Fecha de consulta: 27 de diciembre de 2016].

CAPÍTULO SEXTO

proveedor¹¹¹, con lo cual no sería lícito ofrecer al cliente garantías totales en cuanto a la integridad de sus datos dentro de un entorno digital y en red. Pero ello no obsta para que el proveedor deba adoptar las precauciones en cuanto a seguridad de los datos que le son exigibles como parte de su deber de diligencia profesional. El hecho de que el servicio se preste al cliente sin contraprestación económica no le eximirá de esta responsabilidad, aunque sí podrá tener un carácter moderador sobre el alcance de la indemnización.

3.3.2- La confidencialidad de los datos del cliente y las solicitudes de acceso de terceros

Hemos mencionado ya que la confidencialidad, junto con la integridad y la disponibilidad, integran los fundamentos de la seguridad de la información. Por ello, tras el análisis de la característica de la integridad, abordaremos la problemática de la confidencialidad, con especial atención a las referencias contractuales sobre revelaciones de información migrada por clientes *cloud* bajo requerimiento al proveedor por parte de autoridades legítimas.

En primer lugar, determinaremos el contenido del concepto de confidencialidad. Encontramos su definición legal en el derogado artículo 4 del Reglamento (CE) 460/2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, que entiende la confidencialidad como "la protección de las comunicaciones o de los datos almacenados contra la interceptación y la lectura de los mismos por personas no autorizadas".

A nuestro parecer, y tal como hemos predicado de la integridad, la confidencialidad de los datos almacenados o transmitidos en sistemas informáticos es una cualidad de la seguridad de los datos que debe mantenerse durante todo el ciclo de procesamiento de esa información, es decir, con una duración que abarque desde el momento en que se introduce en un sistema hasta que se produce su borrado definitivo¹¹².

111 Según el art. 1105 del Código Civil: "Fuera de los casos expresamente mencionados en la ley, y de los en que así lo declare la obligación, nadie responderá de aquellos sucesos que no hubieran podido preverse, o que, previstos, fueran inevitables".

112 Sin embargo, esta es una idea no extendida, como sucede con el Anteproyecto de Código Mercantil, que en su art. 440-1.4 limita en el tiempo la obligación post-contractual de confidencialidad a dos años desde la terminación de la relación contractual, aunque permitiendo siempre el pacto en contrario: "Salvo pacto en contrario, el deber de confidencialidad continuará tras la terminación del contrato durante un plazo de dos años". Cabe destacar que el Anteproyecto recoge *ex novo* la cláusula de confidencialidad como opción de pacto entre las partes, y diferenciada de la obligación de confidencialidad nacida en la fase preparatoria. En los contratos de adhesión, tengamos en cuenta que raramente se permitirá al cliente la suscripción de un plazo mayor

CAPÍTULO SEXTO

Tras el estudio de diversos contratos *cloud*, no hemos encontrado proveedores que extiendan la obligación del proveedor de mantener la confidencialidad de los datos más allá de la terminación del contrato y que abarque el plazo que comprende desde el momento del fin de la relación contractual hasta que ha tenido lugar el borrado seguro de la información¹¹³. Sería recomendable, bajo nuestro punto de vista, que se prolongase este deber, como mínimo, hasta que se haya hecho efectivo el borrado de los datos una vez facilitada la portabilidad de estos a otro proveedor o su devolución al cliente, especialmente si se trata de datos de carácter personal o con potencial valor comercial. Nosotros consideramos que esta sería la regulación idónea en los contratos interempresariales, especialmente por la importancia de la información empresarial como activo y por la posición del pequeño empresario como parte contractualmente más débil, susceptible de quedarse en posición de indefensión de sus intereses.

Como hemos apuntado, la naturaleza de los datos y las funcionalidades del concreto servicio de computación en la nube serán aspectos relevantes a efectos de determinar la existencia de tal deber de confidencialidad, y su subsistencia una vez terminado el contrato. A falta de previsión legal, únicamente podrán exigirse responsabilidades en relación a la confidencialidad de los datos atendiendo a la culpa o negligencia en la adopción de medidas de seguridad, a la letra del contrato y a la eventual cobertura legal que puedan tener los datos migrados en función de su contenido (privacidad, secreto de empresa, propiedad intelectual e industrial, etc.).

Tal y como hemos afirmado respecto de la integridad de los datos, puede predicarse la existencia de la obligación de confidencialidad en servicios *cloud* que se presten sin contraprestación dineraria por parte del cliente, ya que tal confidencialidad de la información deriva de la propia naturaleza del contrato *cloud*.

durante el cual sea exigible al proveedor el deber de confidencialidad. Pero la regulación del deber de confidencialidad de la información migrada, como parte integrante de la seguridad de los datos, es, en nuestra opinión, inherente a la naturaleza del contrato de alojamiento de datos, en cuanto estos datos están alojados en sistemas *cloud*. Sin embargo, pese a nuestro posicionamiento, en la regulación de las obligaciones del proveedor del contrato de alojamiento de datos efectuada por los artículos 532-12 y 532-13 del Anteproyecto, no se menciona el deber de confidencialidad del proveedor respecto de los datos alojados ni eventuales usos no autorizados de los datos o de su publicación, sino que únicamente se le exige su conservación.

113 En cuanto a la protección de datos personales, es la misma Ley Orgánica de Protección de Datos de Carácter Personal (y el futuro Reglamento europeo, cuando sea de aplicación) la norma que garantiza la adopción de medidas específicas que aseguren su confidencialidad. Para más información al respecto, ver el capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal", en este mismo trabajo.

CAPÍTULO SEXTO

Es frecuente que el proveedor se reserve, a través de las condiciones generales, el derecho de acceder a los datos para solucionar eventuales problemas técnicos, o para comprobar la adecuación del comportamiento del cliente y de la pertinencia de sus contenidos a las disposiciones contractuales (en especial, a las PUA) y legales¹¹⁴. A nuestro parecer, este tipo de cláusulas son legítimas, e incluso pueden considerarse como objeto del deber de diligencia del proveedor de garantizar la continuidad y seguridad del propio servicio y en beneficio del resto de usuarios. Asimismo, el proveedor de servicios de computación en la nube deberá responder por las revelaciones de datos confidenciales de clientes efectuadas por sus empleados, de acuerdo con los artículos 1902 y 1903 del Código Civil¹¹⁵.

Es relevante la distinción entre los datos confidenciales y los datos revelados por el propio cliente, ya que, en muchos casos, las funcionalidades del servicio *cloud* permiten al cliente "desclasificar" sus datos, al posibilitar compartirlos con otros usuarios del servicio. En estos casos, a él le corresponde, atendiendo a lo suscrito en los contratos de adhesión, la responsabilidad por los contenidos revelados y por los efectos que se deriven de tal decisión¹¹⁶.

Por su parte, el proveedor *cloud* será responsable de mantener las medidas de

114 El famoso caso *Megaupload* y su cierre por infracción de *copyright* a los responsables de ese servicio por una suerte de *culpa in vigilando* parecen haber dejado huella en los contratos de alojamiento de contenidos en servidores remotos. Los proveedores a menudo aprovechan la inclusión de esta cláusula no solo para eximirse de responsabilidad por los contenidos almacenados por el usuario, sino para tener otra vía más para proveerse de acceso a su información. Sin embargo, es el proveedor quien posee los mecanismos técnicos capaces de revelar el uso fraudulento del servicio por un usuario, con lo cual no deja de ser legítimo ese acceso en beneficio del resto de usuarios, del propio proveedor e incluso del interés general.

115 Art. 1902 del Código Civil. "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado". Art. 1903 del Código Civil. "La obligación que impone el artículo anterior es exigible, no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder. (...) Lo son igualmente los dueños o directores de un establecimiento o empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones".

116 Veamos un ejemplo de cláusula de confidencialidad extractada de un contrato de adhesión propuesto por servicios de Microsoft que permiten compartir archivos entre usuarios: "¿Quién puede acceder a mis contenidos? Usted tiene el control inicial sobre quién puede acceder a sus contenidos. Sin embargo, si usted comparte sus contenidos en áreas públicas de los servicios, a través de funcionalidades que así lo permitan, o en áreas en las que otros usuarios que ud. haya elegido puedan acceder a ellos, ud. accede, renunciando a cualquier compensación, a que cualquiera con quien ud. ha compartido sus contenidos pueda utilizarlos, guardarlos, reproducirlos, distribuirlos, exhibirlos y transmitirlos de acuerdo con su uso de estos servicios y de otros productos o servicios licenciados por Microsoft. Si ud. no quiere otorgar estas facultades a otros usuarios del servicio, no utilice estos servicios para compartir sus contenidos". (Traducción propia del original en inglés). Cláusula extractada de las condiciones generales para servicios de Microsoft [en línea]. Disponible en: <<http://windows.microsoft.com/en-us/windows/microsoft-services-agreement>>. [Fecha de consulta: 23 de noviembre de 2016].

CAPÍTULO SEXTO

seguridad adecuadas para que no se produzcan interferencias o accesos no autorizados en datos de los usuarios. En la mayoría de ocasiones median acuerdos recíprocos de confidencialidad que imponen restricciones de divulgación de información a la empresa cliente sobre datos confidenciales a los cuales haya podido tener acceso. En estos casos, el empresario cliente será responsable ante el proveedor por incumplimiento contractual del 1101 del Código Civil¹¹⁷, cuando suponga una infracción de la política de uso adecuado, y ante el perjudicado por una actuación que dará lugar a la responsabilidad extracontractual del artículo 1902 del Código Civil. En su caso, el empresario cliente de servicios *cloud* será responsable por aquellas divulgaciones de datos confidenciales efectuadas por el personal que esté a su cargo, de acuerdo con los mencionados artículos 1902 y 1903 del Código Civil.

Otro aspecto importante de relacionado con la confidencialidad de los datos almacenados en sistemas *cloud* son las solicitudes de datos por autoridades judiciales o investigadoras. La mayoría de contratos recogen las circunstancias en que el proveedor revelará los datos de clientes almacenados en su nube en caso de solicitudes de autoridades¹¹⁸. En función del proveedor, las justificaciones para la entrega de datos de clientes a autoridades pueden ser más o menos restrictivas.

Al respecto, los expertos en contratos de la *Cloud Computing Strategy* de la Comisión Europea aluden a la falta de la precisión de la expresión "orden válida" al mencionar el requerimiento de datos por parte de autoridades, y a que debe distinguirse entre si el origen de la orden es judicial o si proviene de otras autoridades (investigadoras, políticas, etc.)¹¹⁹. Según manifiestan, la locución "orden

117 Art. 1101 del Código Civil. "Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas".

118 Las condiciones del servicio *G-Suite* de Google definen el término "Solicitud de terceros": "hace referencia a una solicitud de un tercero para el acceso a registros relacionados con el uso de los servicios por parte de un usuario final. Las solicitudes de terceros pueden ser una orden de búsqueda legal, una providencia de tribunal, una citación, otra orden legal válida o el consentimiento por escrito del usuario final mediante el que se permite la divulgación". En todo caso, deberemos atender a la letra del contrato para determinar sobre quién recae la discrecionalidad de revelar datos de usuarios finales en caso de peticiones realizadas por entidades que carezcan de autoridad legal o judicial. Condiciones del servicio *G-Suite* de Google [En línea]. Disponible en: <https://gsuite.google.com/intl/es/terms/2013/1/premier_terms.html> [Fecha de consulta: 16 de enero de 2017].

119 El informe, titulado "*Data Disclosure and Integrity Discussion Paper*" fue debatido en la reunión de fecha de 30 de abril de 2014, y el resultado de este debate se halla en la *Synthesis* de 30 de abril de 2014. El contenido de este informe, así como la síntesis y otras reuniones de expertos en contratos de computación en la nube, están disponibles en la página web de la Comisión Europea. <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>.

CAPÍTULO SEXTO

válida" no equivale a orden "vinculante", "coercitiva" o "ejecutable". El proveedor del servicio es quien está en posición de verificar, cuando le llega la petición, que el procedimiento jurídico de requerimiento de datos sea legalmente adecuado, y que no se puedan cometer potenciales abusos con sus clientes.

Como reconocen algunas instituciones españolas, el papel de los proveedores en cuanto a información de estas peticiones a los usuarios es crucial¹²⁰. Algunos proveedores, por su parte, han manifestado que no siempre se podrá garantizar la información previa del cliente afectado por el requerimiento, sino solo en los casos en los cuales la orden de la autoridad competente solicitante lo permita¹²¹.

Por lo expuesto, puede cuestionarse la validez general de las cláusulas del proveedor que le autorizan a la aportación de información a autoridades "competentes" previo requerimiento¹²². Para que sean válidas bajo la normativa

[Fecha de consulta: 6 de junio de 2017].

120 La propia ENISA consideró en 2009 como alto el riesgo de solicitudes de acceso de datos alojados en las nubes por parte de jurisdicciones extranjeras. ENISA, *Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información*, [en línea], 2009. Disponible en: <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file>. [Fecha de consulta: 13 de marzo de 2017].

121 Así lo declaró el director administrativo de *Microsoft UK*, Gordon Frazer en cuanto se le preguntó si Microsoft podía garantizar que los datos almacenados en centros de datos ubicados en la UE no dejarían al Espacio Económico Europeo bajo requerimiento de autoridades con potestades otorgadas por la *Patriot Act*. Noticia disponible en: <<http://www.zdnet.com/article/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/>>. [Fecha de consulta 4 de agosto de 2016]

122 De vuelta a la relación contractual, las estipulaciones sobre el procedimiento de atención a estas solicitudes divergen según el proveedor: algunos afirman que accederán a los requerimientos de manera inmediata y sin restricciones, como los términos de uso del software como servicio de almacenamiento "*iCloud*" del proveedor Apple: "Apple se reserva el derecho a tomar las medidas que determine necesarias o convenientes para hacer cumplir y/o comprobar el cumplimiento con cualquier disposición de este contrato. Usted reconoce y acepta que Apple, sin responsabilidad para usted, puede acceder, usar, conservar y/o revelar la información y el contenido de su cuenta a las autoridades policiales, funcionarios de gobierno, y/o terceros, en la medida que Apple determine necesaria o conveniente, si así se le solicita legalmente o en la creencia de buena fe de que dicho acceso, uso, revelación o conservación es razonablemente necesario para: (a) cumplir procesos o solicitudes legales; (b) hacer cumplir este contrato, incluyendo la investigación de cualquier posible infracción relacionada con las mismas; (c) detectar, impedir o de otro modo solucionar problemas de seguridad, fraudes o problemas técnicos; o (d) proteger los derechos, la propiedad o la seguridad de Apple, sus usuarios, un tercero o el público conforme a lo que exija o permita la legislación". Como podemos observar, las solicitudes a las que hacen referencia este y otros proveedores provienen de mandatos judiciales o de autoridades investigadoras (policiales, tributarias, etc.). En este caso, el proveedor parece ir más allá y someter cualquier decisión sobre revelación de los datos a autoridades a su libre discreción, incluso a terceros que no tengan la calificación de autoridad, basándose en justificaciones indeterminadas y puede que subjetivas, como los "motivos razonables" o de "buena fe". Otros, en cambio, salvaguardan más al cliente y se comprometen a notificarle la existencia de ese requerimiento, a menos que se prohíba tal comunicación. Por ejemplo, la declaración de privacidad de los servicios en línea de Microsoft:

CAPÍTULO SEXTO

española y en relación a ciudadanos españoles, será necesario que ese requerimiento consista en una orden del órgano judicial competente redactada bajo el amparo legal de la normativa específica reguladora de los derechos a la intimidad personal y familiar, al secreto de las comunicaciones y a demás derechos fundamentales que puedan verse afectados, puesto que estas medidas deben adoptarse con las suficientes garantías legales¹²³.

3.3.3.- Política de seguridad. Custodia de los datos.

Como se ha mencionado, la fuente de la obligación del proveedor de incorporar medidas de seguridad en los sistemas puede considerarse, por una parte, inherente a la naturaleza del contrato¹²⁴ y, por otra, resultado de la imposición legal de la normativa sobre privacidad, en cuanto a la seguridad de datos personales (art. 9 LOPD¹²⁵). Igualmente, la propia Ley de Servicios de la Sociedad de la Información

"Microsoft no revelará datos del cliente fuera de Microsoft, o sus filiales y empresas afiliadas, excepto (1) si usted lo solicita, (2) con el permiso de un usuario final, (3) como se describe aquí o en su(s) acuerdo(s), (4) en caso de que así lo requiera la legislación vigente. Microsoft no revelará datos del cliente a la policía a menos que así lo exija la ley. En caso de que los cuerpos y fuerzas de seguridad del Estado se pongan en contacto con Microsoft a fin de solicitar datos del cliente, Microsoft intentará instar a la autoridad competente a solicitarle los datos directamente a usted. Si nos vemos obligados a revelar datos del cliente a las autoridades competentes, Microsoft le notificará inmediatamente y le proporcionará una copia de la solicitud a menos que lo prohíba la legislación vigente. Tras la recepción de cualquier otra solicitud de datos del cliente por parte de terceros (por ejemplo, peticiones de los usuarios finales del cliente), Microsoft le notificará con prontitud a menos que lo prohíba la legislación vigente. Si Microsoft no está obligado por ley a revelar los datos del cliente, Microsoft rechazará la solicitud. Si la solicitud es válida y Microsoft podría verse obligado a revelar la información solicitada, Microsoft intentará instar a dicha compañía o persona a solicitarle los datos directamente a usted. (...)". Términos y condiciones del software como servicio de almacenamiento remoto *iCloud*, del proveedor Apple [en línea]. Disponible en: <<http://www.apple.com/legal/internet-services/icloud/es/terms.html>>. Declaración de privacidad de los servicios *online* de Microsoft [en línea]. Disponible en: <<https://www.microsoft.com/privacystatement/es-es/OnlineServices/default.aspx>>. [Fecha de consulta: 28 de diciembre de 2016].

123 Preocupa especialmente el requerimiento de autoridades en aplicación de la *Patriot Act* norteamericana, puesto que las grandes multinacionales que se configuran como principales proveedores del sector de servicios en la nube tienen sede estadounidense y están sometidas a su legislación nacional. Pero la normativa estadounidense tiene aplicación extraterritorial, con lo cual sus requerimientos de acceso a sistemas de computación en la nube alcanzan también a aquellos centros de datos de proveedores norteamericanos ubicados fuera del territorio estadounidense. Consecuentemente, y ante la fuerza expansiva de la norma americana, Europa ha adoptado diferentes medidas recientes en materia de protección de datos, como los requisitos para la transferencia internacional de datos, las cláusulas modelo elaboradas por los Grupos de Trabajo del Artículo 29, el nuevo acuerdo *Shield* y el recientemente aprobado Reglamento Europeo de Protección de Datos, que serán estudiados en el capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

124 Ver capítulo "Objeto, naturaleza jurídica y características de los contratos de computación en la nube".

125 Art. 9 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter

CAPÍTULO SEXTO

exige a los proveedores "de servicios de correo electrónico y similares" la obligación de informar a sus clientes sobre las medidas de seguridad que apliquen (art. 12 bis, apartados 2 y 5), obligación que, a nuestro parecer, es extensible a proveedores servicios *cloud* que impliquen el alojamiento remoto de información y a quienes les resulte aplicable la LSSI¹²⁶.

En el sector de la computación en la nube, el proveedor suele implementar medidas de seguridad en diferentes áreas: a) seguridad física de la infraestructura y las instalaciones que contienen los centros de datos; b) seguridad de red (implementación de cortafuegos y otras tecnologías que aseguren los accesos al servicio desde la red global); c) seguridad lógica (software de protección ante ataques al sistema y de prevención o paliación de errores); d) segregación de datos; e) encriptado de información a través de algoritmos; y f) políticas de replicado de datos o de copias de seguridad¹²⁷. Todos estos aspectos tienen diferentes niveles en su implementación, y por tanto, la cobertura de seguridad puede ser distinta

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

126 Los proveedores de ciertos servicios en la nube establecidos en España parecen estar obligados por la LSSI a informar sobre las medidas de seguridad que apliquen a los servicios prestados. En concreto, el apartado segundo del artículo 12 bis de la LSSI, se establece, en su apartado 2: "Los proveedores de servicios de acceso a Internet y los prestadores de servicios de correo electrónico o de servicios similares deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios". Como vemos, con este artículo se obligaría únicamente a los proveedores *cloud* de aplicaciones de correo electrónico o similares a que informen de las medidas de seguridad que han adoptado. Quedará a discrecionalidad del juez la interpretación sobre si los servicios de computación en la nube que no consistan en prestaciones de correo electrónico tienen la suficiente semejanza con el servicio de correo electrónico, y, consecuentemente, considerar al proveedor obligado por este deber de información sobre seguridad. El apartado 5 del art. 12 bis de la LSSI dispone lo siguiente: "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". Como vemos, la Ley en ningún momento configura esta obligación de información como parte de la fase precontractual o contractual del servicio, ni que esa información deba ser "clara, comprensible o inequívoca", sino únicamente exige su accesibilidad y disponibilidad por el cliente a través de la web del proveedor. En opinión de los expertos en contratos de la *Cloud Computing Strategy* de la Comisión Europea, a la cual nos adherimos, las medidas de seguridad adoptadas por el proveedor deberían reflejarse en la información precontractual y en el contrato. *Discussion paper on Data Disclosure and Integrity* [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 29 de diciembre de 2016].

127 MARCHINI, Renzo, *op. cit.*, pág. 24.

CAPÍTULO SEXTO

dependiendo de las medidas concretas adoptadas en relación a estas áreas.

Podemos definir las políticas de seguridad como aquel conjunto de compromisos contractuales que asume el proveedor respecto de la seguridad de la información. Es esencial para el cliente empresario obtener una adecuada información sobre estos aspectos, para tener pleno conocimiento de los riesgos que asume al transmitir su información a la nube de ese proveedor, y como parte de su deber de diligencia profesional en cuanto esta migración pueda afectar a su responsabilidad ante terceros¹²⁸.

A continuación analizaremos el carácter contractual de la obligación de adoptar medidas de seguridad para proteger los datos, así como la responsabilidad que se derive de su incumplimiento. Para las cuestiones relacionadas con la privacidad, nos remitimos al capítulo expresamente dedicado a su estudio.

a) El carácter contractual de la obligación del proveedor de establecer medidas de seguridad

Atendiendo al objeto común de la mayor parte de servicios en la nube (en concreto, el almacenamiento y procesamiento remoto de datos del cliente), y a la naturaleza de los contratos de suscripción de esos servicios (como hemos visto en ocasiones similar al depósito¹²⁹), podemos afirmar que el proveedor debe proteger sus sistemas con el fin de garantizar la continuidad de la prestación y la seguridad de los datos alojados por el cliente. Ello deriva de su deber de diligencia profesional. Sin embargo, ello no obsta a que algunos proveedores dispongan cláusulas limitativas de la responsabilidad en relación a la custodia de los datos migrados¹³⁰. Asimismo, el

128 Por otro lado, es comprensible que el proveedor en ocasiones tenga reservas a la hora de informar sobre ciertas características de las medidas de seguridad, no por cuestiones comerciales, sino porque debe evitar desvelar detalles que puedan poner en riesgo la seguridad general del servicio o evidenciar posibles vulnerabilidades del entorno *cloud*. MARCHINI, Renzo, *op. cit.*, pág. 26.

129 Ver capítulo "Objeto, naturaleza jurídica y características de los contratos de computación en la nube".

130 Box define su servicio en sus condiciones generales como: "la solución de almacenamiento alojada facilitada por Box que permite el almacenamiento de contenido, el uso compartido y el procesamiento en línea de archivos, materiales, datos, texto, audio, vídeo, imágenes u otro contenido". No obstante, en las mismas condiciones se exime de la responsabilidad por cualquier incidencia con la integridad de los datos almacenados por el cliente, en los siguientes términos: "Box se esforzará al máximo en prestar los Servicios, pero Box no garantiza ni promete que el contenido que almacene o al que acceda a través de los Servicios no estará sujeto a daños involuntarios, no disponibilidad temporal, corrupción o pérdida. En la medida que lo permita la ley y salvo lo establecido en estas condiciones, Box no será responsable en modo alguno en el caso de que el contenido sea eliminado, corregido o destruido, resulte dañado, se pierda, no se almacene o no se cifre". Términos de servicio de Box [en línea]. Disponible en:

CAPÍTULO SEXTO

cliente, por su parte, debe colaborar en el mantenimiento de la seguridad mediante la adopción de las precauciones que le sean exigibles y un adecuado uso del servicio.

De acuerdo con los modelos de contratos de computación en la nube analizados, podemos afirmar que las cláusulas relacionadas con las medidas de seguridad de los datos pueden clasificarse en varias categorías:

a) Advertencias de seguridad. El proveedor recomienda al cliente la adopción de ciertas cautelas en cuanto a seguridad, manejo y almacenaje de sus propios datos¹³¹. Asimismo, el proveedor ofrece al cliente la posibilidad de personalizar algunos aspectos y funcionalidades (por ejemplo, la compartición de la información con terceros) y de adoptar medidas complementarias que el cliente considere apropiadas de acuerdo con el nivel de criticidad de los contenidos (por ejemplo, la realización de copias de seguridad). El margen de maniobra del cliente respecto de la configuración de aspectos relacionados con la seguridad del servicio podrá variar dependiendo del tipo de servicio contratado y del diseño de ese servicio¹³². Al prevenir al cliente y permitirle configurar algunos aspectos sobre seguridad, el proveedor se exime de la obligación de adoptar esas concretas medidas de seguridad, así como de responder por las consecuencias de la inobservancia de estas recomendaciones por parte del cliente¹³³.

<<https://www.box.com/legal/termsofservice/ES/>>. [Fecha de consulta: 28 de diciembre de 2016]. Ver apartado "Las cláusulas limitativas y exoneratorias de responsabilidad y distribución de riesgos entre las partes. Aceptación de los servicios «tal cual están»".

131 Por ejemplo: "El cliente será responsable de: (i) proteger la confidencialidad de las contraseñas y las cuentas de los Administradores; (ii) gestionar el acceso a las cuentas de los administradores; y (iii) garantizar que el uso de los servicios por parte de los administradores cumpla lo establecido en este acuerdo". Cláusula extractada de los términos y condiciones del servicio *Dropbox para empresas* [en línea]. Disponible en: <https://www.dropbox.com/terms#business_agreement>. [Fecha de consulta: 28 de diciembre de 2016].

132 Queremos recordar, como hemos mencionado en relación con la integridad, que los usuarios de servicios de infraestructura como Servicio (IaaS) y plataforma como servicio (PaaS) poseen más control sobre la seguridad de las aplicaciones. Por esta razón, las filtraciones de datos causadas por errores de codificación del usuario escapan del control sobre seguridad que pueda ejercer el proveedor, porque es el propio usuario quien lo configura y/o diseña, aunque este seguirá obligado a mantener las medidas de seguridad del entorno para proteger los datos de accesos externos no autorizados. Asimismo, el hecho de que un servicio se ofrezca sin contraprestación dineraria puede implicar una diferente distribución de responsabilidades entre las partes, respecto de la seguridad.

133 "Los servicios se proporcionan "tal cual". (...) El cliente será el responsable del mantenimiento de los datos almacenados y de realizar las copias de seguridad pertinentes". Cláusula extractada de los términos y condiciones del servicio *Dropbox para empresas* [en línea]. Disponible en: <https://www.dropbox.com/terms#business_agreement>. [Fecha de consulta: 28 de diciembre de 2016].

CAPÍTULO SEXTO

b) Características de seguridad. Descripción de las medidas técnicas que el proveedor manifiesta tener instauradas en sus sistemas con el fin de satisfacer las necesidades de seguridad y de cumplimiento normativo de los clientes, y las proporciona como parte del servicio de computación en la nube¹³⁴. Estas medidas de seguridad se configuran como objetivos de nivel de servicio, es decir, el proveedor se compromete a tener instalados estos mecanismos, objetivizándose su abstracto deber de diligencia respecto de la instauración de medidas de seguridad. Con la implementación de estas medidas garantiza la obtención de un mínimo nivel de seguridad respecto de los datos del cliente almacenados y del funcionamiento global del servicio¹³⁵.

c) Especificaciones conformes a estándares o "normas de la industria". Son un conjunto de requisitos técnicos que han sido aprobados como estándares¹³⁶ por diferentes organizaciones de normalización¹³⁷.

134 Por ejemplo, el cumplimiento normativo respecto de la normativa en materia de protección de datos de carácter personal.

135 Por ejemplo, la característica de seguridad y cumplimiento normativo del producto en la nube Microsoft Office 365: "Office 365 proporciona capacidades integradas de filtrado de correo no deseado y de malware que permiten proteger los mensajes de correo electrónico entrantes y salientes frente a software malintencionado y ayudan a protegerlo frente al correo no deseado. No necesita configurar ni mantener tecnologías de filtrado, que se habilitan de forma predeterminada, pero puede realizar personalizaciones de filtrado específicas de la compañía". Condiciones de servicio de Microsoft Office 365 [en línea]. Disponible en: <<https://technet.microsoft.com/es-es/library/dn532171.aspx>>. [Fecha de consulta: 29 de noviembre de 2016].

136 Los estándares son documentos con especificaciones técnicas de adopción voluntaria por los proveedores y fabricantes de productos tecnológicos hardware y software. Se elaboran consensuadamente entre miembros de la industria, administraciones y usuarios. Estos estándares pueden ser estándares *de facto* (tienen un uso generalizado derivado de la amplia comercialización de estos productos por empresas líderes en el sector), o estándares institucionalizados (reconocidos como tales por entidades de normalización, como la *International Standard Organization ISO*). Asimismo, existen diferentes categorías de estándares aplicables a tecnología *cloud*: de procesos técnicos, de componentes, de formatos de archivo, de *interfaces*, de seguridad, etc. (Definición propia.). Para más información sobre estándares en entornos de la nube, podemos acudir a la web <http://cloud-standards.org/wiki/index.php?title=Main_Page>. [Fecha de consulta: 22 de mayo de 2015]. A mayor abundamiento, podemos mencionar que el *Cloud Standards Customer Council*, en el año 2015, publicó el informe *Security for Cloud Computing. Ten Steps to Ensure Success*, y también una útil guía para clientes de servicios *cloud*, con indicaciones sencillas para asegurarse de que un proveedor cumple con las medidas de seguridad esenciales. Disponibles respectivamente en: <<http://www.cloud-council.org/deliverables/CSCC-Cloud-Security-Standards-What-to-Expect-and-What-to-Negotiate.pdf>> y <<http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf>>. [Fecha de consulta: 28 de noviembre de 2016].

137 Un ejemplo sería la adopción del estándar para seguridad en la nube *ISO/IEC 27018*. La *Cloud Security Alliance*, en colaboración con el *International Standard Organization (ISO)/IEC's Joint Technical Committee 1/Sub Committee 27 (JTC 1/SC 27)*, ha desarrollado este estándar

CAPÍTULO SEXTO

Ya se deba a la diversidad de estándares o a la evolución constante de la técnica, las cláusulas contractuales de servicios *cloud* comúnmente asumen la adopción de estándares de seguridad, aunque no suelen concretar cuáles son esas medidas concretas ni a qué estándares se acogen¹³⁸. El contenido de estas cláusulas, a nuestro parecer, va más allá de ser una mera manifestación de buenas intenciones o del principio de buena fe contractual, y configura una verdadera obligación contractual, consistente en la adopción de determinadas medidas de seguridad que se configura, bajo nuestro punto de vista, como una obligación de resultado, ya que no solo consiste en adoptar tales medidas, sino en que se cumplan y ejecuten con rigor. Obligación de resultado que no solo es predicable respecto de las medidas de

internacional de confidencialidad de los datos personales en la nube, adoptado por alguna de las empresas referentes del sector, como *Microsoft*. Otro ejemplo sería el del reciente estándar europeo *EuroCloud Star Audit*, presentado en España en enero de 2015, este estándar ha sido creado por la asociación *EuroCloud Europe*, integrada por empresas europeas de tecnologías *Cloud Computing* y *Big Data*. A diferencia de otros estándares internacionales, la certificación *EuroCloud Star Audit* se adapta mejor a las exigencias de la normativa europea, más estrictas en cuanto a seguridad y privacidad de los datos que la normativa de otros estándares como el *ISO 27001/27002* o el *ISAE340*. [En línea]. Disponible en: <<https://eurocloud-staraudit.eu/home/value.html>>. [Fecha de consulta: 28 de diciembre de 2016]. Organizar estos estándares es una de las tareas que se ha propuesto la Comisión Europea, a través de la *Cloud Computing Strategy*. Para esta tarea, ha colaborado, entre otros representantes del sector, con la *European Union Agency for Network and Information Security* (ENISA). En enero de 2016 la presentación de los resultados de la segunda fase de coordinación de estándares para *Cloud Computing*. Estos resultados son cuatro informes con diferentes contenidos respectivamente: las necesidades del usuario, el código abierto, la interoperabilidad y la seguridad, y la evaluación del desarrollo de la adopción de estándares en el sector. Disponibles en: <<http://csc.etsi.org/>>. [Fecha de consulta: 29 de noviembre de 2016]

138 Como ejemplo, esta cláusula extractada de los términos y condiciones, versión en castellano, del SaaS de pago por almacenamiento *Dropbox para Empresas*: "Dropbox utilizará, como mínimo, las medidas de seguridad técnicas y organizativas estándar del sector para transferir, almacenar y procesar los datos del cliente. Estas medidas están diseñadas para proteger la integridad de los datos del cliente y salvaguardarlos contra cualquier acceso, uso o procesamiento no autorizado de los datos del cliente. (...)". Condiciones del servicio *Dropbox para empresas* [en línea]. Disponible en: <https://www.dropbox.com/terms#business_agreement>. [Fecha de consulta: 28 de diciembre de 2016]. En ocasiones, los proveedores son más transparentes en cuanto a la seguridad adoptada. Por ejemplo, *Amazon Web Services* recoge en su web los estándares y prácticas recomendadas que adopta. [En línea]. Disponible en: <<http://aws.amazon.com/es/compliance/>>. [Fecha de consulta: 29 de noviembre de 2016]. Además, va publicando periódicamente un informe sobre cómo protege su nube. En concreto, nos referimos al informe publicado en agosto de 2016. [En línea]. Disponible en: <<https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf>>. [Fecha de consulta: 29 de noviembre de 2016]. Sin embargo, hay proveedores que consideran que proporcionar detalles a potenciales clientes sobre políticas y prácticas de seguridad, sobre todo en infraestructuras compartidas, puede comprometer la seguridad del sistema y revelar vulnerabilidades. Cuando se trata de contratos negociados (no de adhesión), ciertos clientes tienen más posibilidades de averiguar y negociar detalles específicos, visitar centros de datos e instalaciones, entrevistarse con el personal técnico, etc. Siempre, claro está, previos acuerdos de confidencialidad.

CAPÍTULO SEXTO

seguridad que se adoptan para proteger los datos de carácter personal sino también, según nuestro criterio, en aquellas destinadas a proteger los datos almacenados en el servicio y la continuidad de éste¹³⁹.

Si la política de seguridad se adecua a algún concreto estándar, por ejemplo, el estándar ISO/IEC 27017, el cliente de ese servicio *cloud* tiene una referencia sobre las medidas de seguridad implementadas, aunque será preferible que el proveedor pueda demostrar este cumplimiento, por ejemplo, mediante una certificación que acredite que la implementación de estándares ha sido auditada por un evaluador externo reconocido, al ofrecer mayores garantías que un simple compromiso del propio proveedor sobre la implementación de medidas de seguridad¹⁴⁰.

139 La Audiencia Nacional ha reconocido en diferentes sentencias que la obligación de implementar medidas de seguridad para proteger datos de carácter personal es una obligación de resultado, aunque reconoce que esta exigencia de resultado tiene que interpretarse en cada caso. A modo de ejemplo, su sentencia de 28 de junio de 2006, Sala de lo Contencioso Administrativo, fundamento cuarto: "(...) se impone, en consecuencia, una obligación de resultado, consistente en que se adoptan las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros...la recurrente es, por disposición legal una deudora de seguridad en materia de datos,(...), siendo insuficiente con acreditar que adopta una serie de medidas, pues es también responsable de que las mismas se cumplan y se ejecuten con rigor", y su Sentencia de 26 de abril de 2012, Sala de lo Contencioso Administrativo, fundamento Cuarto: "esta Sala se ha pronunciado en diversas ocasiones entendiendo que se trata de una infracción de resultado y que no basta, entonces, con la adopción de cualquier medida, pues deben ser las necesarias para garantizar aquellos objetivos que marca la normativa específica precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva, por esta razón de nada sirve que se aprueben unas instrucciones detalladas sobre el modo de proceder si después estas no se llevan a la práctica de modo efectivo" y que "esta exigencia de resultado no debe interpretarse de modo maximalista (...) sino acomodado a la realidad de cada caso". Disponible en: <<http://www.asesoriayempresas.es/jurisprudencia/JURIDICO/139623/sentencia-an-de-26-de-abril-de-2012-proteccion-de-datos-infraccion-de-la-junta-de-extremadura>>. Ver apartado "Responsabilidad directa del proveedor: limitaciones y exoneraciones. (...)", en este mismo capítulo.

140 El cumplimiento con estándares del sector suele ser publicitado por el propio proveedor, como garantía de confianza. Además, la adopción de estas medidas puede servir como prueba en relación al cumplimiento de las exigencias legales en materia de protección de datos. Las series de estándares ISO/IEC 27000 incluyen los estándares de seguridad de la información publicados por dos organismos de referencia: la *International Organization for Standardization* (ISO) y la *International Electrotechnical Commission* (IEC). El estándar de esta serie especialmente dedicado a la seguridad de la información en la nube es el estándar ISO/IEC 27017, publicado a finales de 2015, sobre controles de seguridad específicos para *Cloud Computing*. Ejemplos de proveedores *cloud* certificados de acuerdo con el cumplimiento del estándar ISO/IEC son *Amazon*, en relación a sus servicios *Amazon Web Services* (<<https://aws.amazon.com/es/compliance/iso-27017-faqs/>> [Fecha de consulta: 28 de diciembre de 2016].) o *Microsoft* respecto de su servicio *Microsoft Azure* (<<https://azure.microsoft.com/en-us/blog/microsoft-obtains-new-cloud-centric-iso-27017-certification/>>, [Fecha de consulta: 28 de diciembre de 2016]). Más información en el sitio web de los estándares ISO/IEC [en línea]. Disponible en:

CAPÍTULO SEXTO

Como veremos más adelante, el proveedor suele reservarse el derecho a modificar unilateralmente el contrato, lo cual puede significar la introducción de cambios en las políticas de seguridad¹⁴¹.

b) La seguridad de los sistemas y el plan de emergencia ante incidentes de seguridad como obligaciones de resultado

Como hemos mencionado anteriormente, la calidad de los recursos proporcionados por el proveedor (por ejemplo, el almacenamiento remoto) puede suponer la custodia de los datos del cliente de manera segura y que estén accesibles cuando este los requiera. El deber de custodia de los datos migrados corresponde al prestador *cloud*, como bien apuntan algunos autores en relación a contratos similares¹⁴², por razón de la recepción y tenencia de bienes ajenos, al derivarse de la naturaleza de los servicios *cloud* en los que tiene lugar la transmisión de datos digitales del cliente a sistemas del proveedor para su almacenamiento y custodia¹⁴³.

Este deber de custodia de los datos del cliente se concreta en dos obligaciones. Por un lado, en la obligación de adoptar las medidas y protocolos de seguridad que garanticen al máximo la protección de las instalaciones físicas y lógicas que sirven de soporte al almacenamiento; y por otro lado, que los datos del cliente permanezcan íntegros y confidenciales hasta el momento de su restitución¹⁴⁴.

Igual tratamiento que las anteriores actividades preventivas debe recibir, bajo nuestro punto de vista, la adopción de un plan de gestión de incidentes de seguridad, con el fin de recuperar, ante incidencias de cualquier índole, la operativa habitual

<<http://www.iso27001security.com/html/27017.html>>. [Fecha de consulta: 28 de diciembre de 2016].

141 Ver capítulo "Modificación, suspensión y extinción del contrato de servicios de computación en la nube".

142 En relación al contrato de *hosting*, YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet, Hosting y búsqueda*, Navarra, 2012, pág. 344.

143 Ver capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube", en especial, el apartado dedicado a la similitud entre el contrato *cloud* y el depósito tradicional.

144 A continuación, una cláusula extractada del acuerdo *online* del software como servicio *G-Suite* de Google: "Las instalaciones que se empleen para almacenar y procesar datos del cliente deberán cumplir con normas de seguridad razonables y en ningún caso podrán ser inferiores a las normas de seguridad de las instalaciones en las que Google almacena y procesa información similar propia. Google ha implementado como mínimo los sistemas y procedimientos estándar del sector para garantizar la seguridad y confidencialidad de los datos del cliente, protegerlos contra amenazas o riesgos previstos para la seguridad o integridad de dicha información, y evitar accesos no autorizados e impedir su uso". [En línea]. Disponible en: <<https://www.google.com/apps/intl/es/terms/sla.html>>. [Fecha de consulta: 29 de diciembre de 2016].

CAPÍTULO SEXTO

del sistema y los datos afectados a la mayor brevedad posible¹⁴⁵. Su no adopción supone una infracción del deber de diligencia profesional¹⁴⁶. Las directrices de la Comisión Europea recomiendan a los proveedores que determinen en el acuerdo de nivel de servicio parámetros que permitan objetivizar esta obligación abstracta, entre los que destacan el porcentaje de errores corregidos durante un determinado período, y la determinación de algún tipo de mecanismo que permita al cliente realizar un seguimiento del estado de recuperación del sistema¹⁴⁷.

Como hemos apuntado, en los servicios IaaS (infraestructura como servicio) y PaaS (plataforma como servicio), el usuario tiene capacidad para configurar los procesos relacionados con las capas inferiores de la arquitectura en la nube, en las que se integran medidas de seguridad tanto físicas como lógicas. En cambio, en los SaaS (software como servicio), la prestación se centra en las funcionalidades, y los aspectos de seguridad vienen configurados de origen por el proveedor, con lo cual el usuario tiene una mínima maniobrabilidad sobre medidas de seguridad, pudiendo configurar, como mucho, unos pocas preferencias en cuanto a privacidad o compartición de información con terceros. Así pues, el deber de diligencia del proveedor se corresponderá con aquellos aspectos de seguridad que tenga bajo su ámbito de control, y se distribuirá con la diligencia que debe mostrar el cliente en el uso del servicio y respecto de las advertencias de seguridad que pueda efectuar el proveedor al respecto. Así, el cliente en ocasiones podrá personalizar ciertos aspectos que pueden afectar al entorno de seguridad del servicio (compartición de información con terceros, encriptado, etc.), y deberá controlar las claves de acceso y

145 En las recomendaciones del *Cloud Council* a la hora de contratar servicios *cloud* se afirma: "el proceso de idear un plan de recuperación en caso de desastre empieza con la identificación de aplicaciones, servicios y datos prioritarios, y la determinación par cada uno de ellos del tiempo aceptable antes de que se produzca un importante impacto en la operativa empresarial del cliente. (...) Por ejemplo, en ocasiones puede ser importante mantener los datos accesibles que su replicado". (Traducción propia). *Practical Guide to Service Level Agreements*, V2.0 [en línea]. Disponible en: <http://www.cloud-council.org/CSCC_Practical_Guide_to_Cloud_Service_Agreements_Version_2.0.pdf>. [Fecha de consulta: 29 de diciembre de 2016]

146 En el mismo sentido, SCHREIDER, Tari, "White Paper. The Legal Issues of Disaster Recovery Planning", *Disaster Recovery Journal*, 1996, [en línea]. Disponible en: <<http://lbr.covalentwords.com/assets/docs/348.pdf>>. [Fecha de consulta: 12 de diciembre de 2015].

147 COMISIÓN EUROPEA. *Cloud Service Level Agreement...*, *op. cit.* (Traducción propia). Por ejemplo, en el acuerdo de nivel de servicio del software como servicio *Microsoft Dynamics CRM*, el proveedor *Microsoft* se compromete a notificar las incidencias y a permitir su seguimiento a través de la puesta a disposición de sus clientes del denominado "panel de estado del servicio". Condiciones de *Microsoft Dynamics CRM* [en línea]. Disponible en: <<https://technet.microsoft.com/es-es/library/jj134081.aspx>> [Fecha de consulta: 29 de diciembre de 2016].

CAPÍTULO SEXTO

otros códigos de seguridad de los que pueda disponer para ejecutar funcionalidades del servicio.

En cuanto al contenido de las cláusulas sobre seguridad de los sistemas de computación en la nube, cabe comentar que la obligación del proveedor de implementar medidas de seguridad robustas (sean o no consideradas estándares del sector) y actualizadas no deriva únicamente de su inclusión en el contrato.

En la ausencia de tales condiciones, se entendería implícito en el contenido de la relación obligatoria que comprende el contrato *cloud*, atendiendo a su objeto, finalidad¹⁴⁸, a los usos de la industria¹⁴⁹ y a la buena fe contractual¹⁵⁰.

El cliente tiene expectativas legítimas en cuanto a la custodia de los contenidos que transfiere o introduce en el sistema del proveedor, puesto que la utilidad de las funcionalidades o capacidades del servicio contratado depende, en gran parte, de la migración, procesamiento y almacenamiento de sus contenidos; y de que estos, a su vez, no hayan sufrido alteraciones no autorizadas, sean

148 La finalidad de la contratación de un servicio de computación en la nube es el suministro al cliente/usuario, a través de la Red, de capacidades informáticas físicamente ubicadas en centros de datos remotos. La recepción por el cliente y/o usuario de este suministro informático es la razón de ser del contrato.

149 La adopción de ciertas medidas que podríamos considerar mínimas (vigilancia de las instalaciones que contienen los centros de datos, cortafuegos, antivirus, controles de acceso a los sistemas, etc....) se integran en las prácticas habituales o usos dentro del sector de servicios tecnológicos y *cloud*. Por otra parte, resulta complicado recopilar cuáles son esas medidas mínimas, puesto que son diversas debido a la variedad de los servicios y a su evolución tecnológica. Para ello existen los estándares y las prácticas recomendadas, aunque son de adopción voluntaria por los proveedores. No obstante, la adopción de medidas mínimas puede no ser suficiente cuando se trate de migrar a la nube pública datos especialmente sensibles o críticos (datos sobre salud, datos empresariales altamente confidenciales, información de abogados sobre los casos de sus defendidos, información de aseguradoras, etc.). Para estos casos, es recomendable obtener del proveedor la información precontractual completa sobre las medidas de seguridad implementadas que garanticen al cliente su capacidad para albergar datos con necesidades especiales de protección; o escoger servicios que se caractericen por tener instaladas medidas de seguridad de alto nivel capaces de garantizar la seguridad los datos delicados de cada uno de sus múltiples usuarios, como una nube privada o comunitaria.

150 En palabras de Díez-Picazo, la buena fe es "aquella conducta social que la conciencia social exige en cada caso conforme a un imperativo ético dado"; pero "solo podrán ser consideradas como obligaciones o como deberes dimanantes de buena fe aquellos que la otra parte puede razonablemente esperar que sean adoptados". En cuanto a fuente de especiales deberes de conducta, la buena fe "da lugar al nacimiento de una serie de deberes especiales de conducta", y puede imponer al deudor de la prestación (en este caso, el proveedor de servicios *cloud*) "la necesidad de realizar comportamientos que eviten lesiones; deberes de llevar a cabo las actividades necesarias para que la prestación sea definitivamente útil (...)". DIEZ-PICAZO, Luís, *Fundamentos de Derecho Civil Patrimonial, Tomo I: Introducción. Teoría del contrato*. 6ª Edición, Navarra, 2013, págs. 61, 63 a 64.

CAPÍTULO SEXTO

confidenciales y estén accesibles bajo petición del cliente y/o usuario.

A grandes rasgos, el *status* del proveedor *cloud* como profesional le obliga a realizar diferentes actuaciones en materia de seguridad, entre las que destacan las siguientes: aislar oportunamente los centros de datos físicos; seleccionar e implementar las medidas técnicas de protección de los sistemas físicos y lógicos y de los datos estáticos y en tránsito, realizar replicados que permitan el suministro ininterrumpido del servicio; y organizar protocolos de actuación en caso de incidencias, junto con una adecuada formación del personal al cargo de tareas relacionadas con la seguridad¹⁵¹. Consideramos estas actuaciones como una obligación de resultado que se entiende cumplida únicamente cuando el proveedor efectivamente ha instalado las medidas de seguridad adecuadas y actualizadas en sus sistemas para proteger los datos y maximizar la continuidad del servicio, y establece y cumple con los protocolos de actuación previstos para casos de incidentes de seguridad.

Sin embargo, esta implementación de medidas no supone una garantía absoluta de que los datos permanezcan siempre inalterados, confidenciales o disponibles, ni de que el servicio esté permanentemente activo, puesto que existen otros factores que escapan del control del proveedor y que pueden alterar la seguridad y la continuidad de la prestación, tales como averías o fallos humanos, ataques informáticos deliberados e inevitables, problemas con subproveedores, intervenciones de autoridades, etc.

La responsabilidad del proveedor *cloud* derivada de incidentes de seguridad dependerá de la efectiva implementación de las medidas de seguridad del servicio (que, como hemos dicho, es una obligación de resultado), de la previsibilidad y evitabilidad de la contingencia, y de las limitaciones y exclusiones de responsabilidad que el cliente pequeño empresario haya podido aceptar a través de las cláusulas contractuales¹⁵².

Para acabar con este apartado, cabe mencionar que existen certificados de

151 Respecto de la relación de *Outsourcing* informático, en opinión de APARICIO VAQUERO, y con la cual coincidimos y consideramos extensible a la contratación *cloud*, la despreocupación del cliente por la gestión de los recursos informáticos de su empresa (mantenimiento, reparaciones, actualización, etc.) dejando en manos de un profesional experto la actividad y el riesgo informáticos, se convierte en causa del contrato, siendo la intención de ambas partes a la hora de contratar el servicio. Al respecto, nos remitimos a APARICIO VAQUERO, Juan Pablo, *La nueva contratación...*, *op. cit.*, pág.105.

152 Ver apartado "Responsabilidad en cuanto a la custodia de los datos y pérdidas accidentales", en este mismo capítulo.

CAPÍTULO SEXTO

cumplimiento de estándares de seguridad que le conceden al cliente una mayor confianza en el servicio prestado por el proveedor¹⁵³. El proceso de expedición de certificados se realiza por terceros independientes al proveedor, y evalúa objetivamente ciertos parámetros de seguridad para determinar en qué grado se cumplen tales parámetros durante la prestación ordinaria del servicio *cloud*. Cuando se haya obtenido el certificado, el proveedor puede publicitarlo como referencia de calidad, y se recomienda que se mencione la entidad que lo concede y el período de validez del certificado¹⁵⁴.

Una vez delimitadas las obligaciones relacionadas con la seguridad del servicio y de los datos migrados, pasamos ahora a analizar la responsabilidad derivada de incidentes de seguridad que afecten a datos del cliente.

c) Responsabilidad en cuanto a la custodia de los datos y pérdidas accidentales

En primer lugar, será indispensable analizar la causa del incidente que ha alterado la seguridad de los datos para determinar las ocasionales consecuencias jurídicas, como la posibilidad de resolver el contrato por parte del cliente y el derecho a obtener una compensación económica por los daños. Así, deberá identificarse si la brecha de seguridad era previsible y/o evitable, si es atribuible a alguna de las partes o a un tercero o, si por el contrario, puede considerarse caso fortuito o fuerza mayor¹⁵⁵. A partir de este punto, y analizando la ley aplicable y la

153 Por ejemplo, la agencia ENISA, grupo de expertos que colabora con la Comisión Europea, ofrece en su sitio web una lista de certificados desarrollados dentro del marco de la *European Cloud Computing Strategy*, entre los que destacan la certificación STAR y los certificados de cumplimiento con los estándares ISO/IEC 27001. [En línea]. Disponible en: <<https://resilience.enisa.europa.eu/cloud-computing-certification>>. [Fecha de consulta: 29 de diciembre de 2016]

154 COMISIÓN EUROPEA. *Cloud Service Level Agreement Standardisation Guidelines* [en línea]. Disponible en: <<https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>>. [Fecha de consulta: 12 de diciembre, 2015]

155 El Fundamento V de la sentencia del Tribunal Supremo de 8 de abril de 2008, Sección 1, distingue los efectos entre caso fortuito y fuerza mayor: "El caso fortuito, que también recoge el artículo 17.8 de la LOE, es todo suceso imposible de prever, o que previsto, sea inevitable y, por tanto, realizado sin culpa del agente, de tal forma que el vínculo de causalidad se produce entre el acontecimiento y el daño sin que en él intervenga como factor apreciable la actividad dolosa o culposa del agente, por lo que, para que tal suceso origine exención de 5 responsabilidad es necesario que sea imprevisible o inevitable, y que, cuando el acaecimiento dañoso fuese debido a incumplimiento del deber relevante de previsibilidad, no puede darse la situación de caso fortuito, debido a que falta la adecuada diligencia por omisión de la atención y cuidados requeridos con arreglo a las circunstancias del caso, lo que hace inaplicable la excepción del art. 1105, al no darse la situación de imprevisibilidad o irresistibilidad requeridas por el precepto. (...) Asimismo tiene declarado esta Sala que "la aplicación del repetido art. 1105 exige que conste acreditada la imprevisibilidad del evento dañoso, cuestión esta, como la previsibilidad, que tiene la cualidad de hecho" (SSTS 2 de febrero 1989; 23 de junio 1990; 2 de febrero de 2006), o, como dice la sentencia de 4 de noviembre de 2004, "desde la óptica casacional, se considera la problemática del caso fortuito y de la fuerza mayor, con

CAPÍTULO SEXTO

letra del contrato, se determinará si cabe reclamar al proveedor por incumplimiento contractual (es decir, ha incumplido la obligación sobre la adopción de medidas de seguridad)¹⁵⁶. A su vez, el proveedor podrá reclamar, en su caso, a otros eventuales responsables de las brechas de seguridad, por ejemplo a otros usuarios que incumplan la política de uso del servicio y accedan a información de otros usuarios, o a subproveedores de capas subyacentes (art. 1904 Código Civil)¹⁵⁷.

Los daños ocasionados por fallos de seguridad en la prestación de servicios de computación en la nube generalmente tendrán carácter patrimonial y/o moral, y afectarán a las características esenciales de la seguridad de los datos migrados: falta de disponibilidad de tales datos por parte de los usuarios autorizados (lo que puede obstaculizar la actividad habitual del empresario cliente) y/o alteraciones de su integridad (pérdidas de información) y confidencialidad (acceso de terceros o puesta en compromiso)¹⁵⁸.

Una vez identificado el problema que ha ocasionado la quiebra en el sistema, forma parte del deber de diligencia profesional del proveedor poner en marcha los protocolos de aislamiento de las áreas afectadas e iniciar los procesos necesarios para remediar la situación¹⁵⁹ y minimizar sus efectos dañinos, cuyo cumplimiento se materializa en la aplicación del protocolo conocido como "*disaster recovery plan*"¹⁶⁰.

En cuanto a los efectos jurídicos de las brechas de seguridad, en la práctica contractual de servicios de computación en la nube son frecuentes las cláusulas de limitación o exención de responsabilidades en relación a la existencia de un deber de

carácter general, como cuestiones de hecho cuya apreciación corresponde al juzgador de instancia"; doctrina que determina la desestimación del motivo en un supuesto en el que la sentencia descarta que no sea previsible un hecho de la construcción en el que intervienen personas específicamente expertas en el estudio y valoración de las condiciones del suelo, de la resistencia y de las previsiones de seguridad y funcionamiento de las edificaciones, máxime cuando el estado de la ciencia y de la técnica en estas materias, hacían posible calcular o prever la aparición de las grietas y su posterior reparación y evitación".

156 Ver apartado "Responsabilidad directa del proveedor: limitaciones y exoneraciones. (...)", en este mismo capítulo.

157 Art. 1904 del Código Civil: "El que paga el daño causado por sus dependientes puede repetir de éstos lo que hubiese satisfecho. (...)".

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

159 HON, W KUAN; W; MILLARD, C, "Negotiated contracts for Cloud Services", *Cloud Computing Law*, (coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 97.

160 Este plan, que suele estar documentado, contiene acciones preventivas para minimizar los riesgos y los efectos de eventuales incidentes graves que puedan comprometer la continuidad de la prestación del servicio. Cuando tiene lugar el percance y se ha evaluado su alcance, se intentará, a la mayor brevedad posible, reparar los equipos que puedan haber resultado afectados, restaurar los contenidos a partir de copias de seguridad y asegurar la disponibilidad operativa del entorno para todos sus clientes.

CAPÍTULO SEXTO

diligencia profesional de custodia de los datos migrados, con lo cual difícilmente el proveedor asumirá responsabilidad absoluta sobre incidencias relacionadas con la seguridad de sus sistemas¹⁶¹.

Consideramos que estas cláusulas son contrarias, al menos en parte, a la propia naturaleza del servicio *cloud*¹⁶² y, que, por ello, debería valorarse su admisibilidad, especialmente en aquellos contratos que, al quedar fuera del amparo de la protección del consumidor, se presume su validez en virtud del principio de la autonomía de la voluntad de las partes puesto que tiene lugar entre profesionales, y que, sin embargo, no han podido ser negociados al tratarse de contratos predispuestos por el proveedor para su suscripción masiva¹⁶³. Además, estas cláusulas no pueden encubrir exenciones de responsabilidad por dolo (en cuyo caso, serían nulas de acuerdo con el art. 1102 del Código Civil¹⁶⁴).

161 Veamos un ejemplo de estas cláusulas de exención de responsabilidad por la custodia de los datos migrados por el cliente: "Box se esforzará al máximo en prestar los servicios, pero Box no garantiza ni promete que el contenido que almacene o al que acceda a través de los servicios no estará sujeto a daños involuntarios, no disponibilidad temporal, corrupción o pérdida. En la medida que lo permita la ley y salvo lo establecido en estas condiciones, Box no será responsable en modo alguno en el caso de que el contenido sea eliminado, corregido o destruido, resulte dañado, se pierda, no se almacene o no se cifre". Condiciones de uso de Box [en línea]. Disponible en: <<https://www.box.com/legal/termsofservice/ES/>>. [Fecha de consulta: 29 de diciembre de 2016].

162 Cuando existen cláusulas contractuales que, aparentemente, contradicen la propia naturaleza jurídica del contrato, en algunas jurisdicciones se aplica la llamada "regla de la cláusula sorprendente". La regla de la cláusula sorprendente aparecía recogida en el artículo 5 del Proyecto de la Ley de Condiciones Generales de la Contratación: "no quedarán incorporadas al contrato las (...) condiciones generales (...) que de acuerdo con las circunstancias y, en especial, con la naturaleza del contrato, resulten tan insólitas que el adherente no hubiera podido contar razonablemente con su existencia". PAGADOR LÓPEZ, Javier, "Condiciones generales y cláusulas abusivas", en *Defensa de los Consumidores y Usuarios. comentario sistemático del texto Refundido aprobado por Real Decreto 1/2007*, (Directores: Rebollo Puig, Izquierdo Carrasco), Madrid, 2011, pág. 1365. El Tribunal Supremo, en sentencia de 7 de octubre de 2007, Sala Primera, afirma en su fundamento tercero que, "en nuestro Derecho, la falta de acogida explícita de la regla de "las cláusulas sorprendentes" en la Ley General de Defensa de Consumidores y Usuarios y en la Ley de Condiciones Generales de la Contratación todo vestigio sobre ellas, y tampoco que carezcan de virtualidad pues, de un lado, existen señales de las mismas en la Disposición Adicional Primera de la Ley primeramente indicada, y de otro, en el ámbito de la Ley de contrato de seguro, dicha pauta late en la prohibición de las cláusulas lesivas para los asegurados, y la doctrina jurisprudencial las ha configurado exclusiva y genéricamente dentro de dicho espacio". En el mismo sentido, la Sentencia de la Audiencia Provincial de Madrid, Sección 11, de 14 de abril de 1992, en la que se entiende que el servicio de aparcamiento lleva implícita, de acuerdo con los usos y buena fe, la vigilancia del vehículo, por ser "integrante de la utilidad o finalidad esencial del producto o servicio". BELLO JANEIRO, Domingo: "Cláusulas de exclusión o reducción de responsabilidad en la Ley General de Consumidores y Usuarios", *Anuario da Facultade de Dereito da Universidade da Coruña*, núm. 2, 1998, pág. 638.

163 En el mismo sentido, y respecto de los contratos de *Outsourcing* informático, APARICIO VAQUERO, Juan Pablo, *La nueva contratación...*, *op. cit.*, pág.103.

164 Art. 1102 Código Civil: "La responsabilidad procedente del dolo es exigible en todas las obligaciones.

CAPÍTULO SEXTO

Respecto de este tipo de cláusulas, habituales en la práctica, hay que señalar de entrada que, en la prestación de servicios *cloud*, y en realidad, en la prestación de servicios relacionados con la técnica informática, la garantía total de la custodia de los datos resultaría, cuanto menos, utópica, debido a los riesgos inherentes a prestaciones que involucran redes y equipos informáticos (averías, problemas con la red eléctrica o con Internet, ataques maliciosos, etc.). Sin embargo, consideramos que el proveedor no debería poder eximirse del deber de diligencia que le corresponde en relación a cualquier incidencia relacionada con la seguridad de los datos únicamente a través de la introducción de cláusulas contractuales de este calibre, ni tampoco fundamentándose en la aceptación por parte del cliente de un servicio *cloud* "tal y como está". Ambos mecanismos (exclusiones o limitaciones de responsabilidad y aceptación del servicio tal y como se presta al cliente) vacían de contenido el deber de diligencia profesional del proveedor. Desafortunadamente, la regulación de las cláusulas abusivas solo tiene como beneficiarios, según la legislación actual, a los consumidores¹⁶⁵.

En este aspecto, y en el estudio de los contratos analizados para este trabajo, hemos observado notables diferencias entre los contratos sujetos a normativa estadounidense y aquellos que se someten a regulación europea¹⁶⁶. Las leyes americanas otorgan un margen más amplio en cuanto a la admisibilidad de exclusiones de garantías y limitaciones de responsabilidad, dando prioridad a aquello pactado, mientras que en Europa, en cambio, las transacciones en las que una parte tiene una posición claramente predominante, como pueden ser los contratos con consumidores o pequeñas empresas y en la contratación a distancia, implican para el proveedor obligaciones legales y cláusulas que pueden quedar invalidadas o que pueden dar lugar a compensaciones, puesto que así aparece regulado en las respectivas directivas sobre estas materias¹⁶⁷.

La renuncia de la acción para hacerla efectiva es nula".

165 Ello no obsta a que los tribunales puedan realizar interpretaciones más flexibles en beneficio del pequeño empresario adherente. 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 este mismo capítulo.

166 BRADSHAW, S; MILLARD, C; WALDEN, I, "Standard contracts for Cloud Services", *Cloud Computing Law*, (Coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 66.

167 Consideramos adecuado hacer unas brevísimas referencias a la legislación contractual norteamericana. El Derecho contractual de los Estados Unidos difiere entre los diferentes Estados, puesto que cada Estado posee regula los diferentes sectores industriales, y posee su propia interpretación jurisprudencial, aunque el *Uniform Commercial Code* ha dotado de cierta uniformidad a las legislaciones nacionales. Por eso, cuando un contrato *cloud* entre empresas remita a una concreta legislación nacional norteamericana, deberemos acudir a lo establecido en la

CAPÍTULO SEXTO

Asimismo, resulta comprensible, en nuestra opinión, que los servicios de pago impliquen más compromisos de responsabilidad en materia de seguridad que los servicios sin contraprestación dineraria por parte del cliente, al igual que, entendiendo la complejidad de los entornos en la nube, no consideramos admisible que el proveedor se vea obligado a asumir la responsabilidad absoluta por la seguridad de los sistemas y de los datos del cliente. Sin embargo, todo ello no es óbice para que los contratos de computación en la nube destinados a consumidores y pequeñas empresas muestren una distribución más equitativa de las responsabilidades en cuanto a la integridad de los datos.

Lo anterior debe ponerse también en relación con la reserva del derecho de modificación unilateral de cláusulas contractuales y la evolución en las tendencias de la industria tecnológica pueden provocar cambios en las políticas de seguridad. Normalmente estos cambios se manifestarán a través de la adopción de medidas de seguridad más robustas y actualizadas y protocolos más estrictos, aunque puede que no siempre sea así, dado que el proveedor podrá valorar otras variables en la decisión sobre qué medidas o protocolos debe implementar, tales como la relación coste-beneficio, o las necesidades de los clientes que mayoritariamente comparten los recursos (empresas, particulares, entidades financieras, administraciones públicas, etc.)¹⁶⁸.

3.4.- El cumplimiento defectuoso y la determinación de *service credits* como indemnización al cliente

Cuando no se alcanzan ciertos objetivos de nivel de servicio, contractualmente se pueden establecer compensaciones para el cliente¹⁶⁹. Más

regulación y jurisprudencia de ese Estado. En cuanto a transacciones internacionales, a la espera del nuevo Tratado de libre comercio entre Estados Unidos y Europa, cabe destacar que no existe, por el momento, una regulación especial de las condiciones generales de contratación en Derecho Internacional Privado. Al respecto, nos adherimos a la opinión de VEGA VEGA: "Por todo ello, la protección del adherente en la esfera internacional debe considerarse a todas luces insuficiente, (...), por lo que se impone como cuestión de lege ferenda nacional o internacional la promulgación de leyes más específicas al respecto (...)". VEGA VEGA, José A. *Contratos electrónicos y protección de los consumidores*. Madrid, 2005, pág. 294.

168 HON, W KUAN; W; MILLARD, C, "Negotiated contracts for Cloud Services", *Cloud Computing Law*, (coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 93.

169 Estas compensaciones no operan con cualquier incumplimiento defectuoso del servicio *cloud*, sino únicamente con aquellos objetivos de nivel de servicio asociados con la concreta compensación. Tampoco operan de manera automática, sino que pueden estar sujetas al cumplimiento de algunas condiciones, como veremos a continuación.

CAPÍTULO SEXTO

concretamente, en casos de falta de disponibilidad del servicio, es habitual que el proveedor incluya una suerte de cláusulas similares a las cláusulas penales que operarán en el caso de que no se alcancen algunos niveles mínimos de calidad de la prestación (siendo este el criterio determinante, y no la causación de un daño por el proveedor)¹⁷⁰.

En los servicios de computación en la nube, estas compensaciones se presentan a modo de "créditos de servicio" (en inglés, *service credits*)¹⁷¹. En el contexto de la computación en la nube, podemos definir las como aquellas compensaciones predeterminadas en el contrato, consistentes en rebajas en futuras facturaciones al cliente por la falta de consecución por el proveedor de ciertos objetivos de nivel de servicio, concretamente de aquellos relacionados con la calidad en el desempeño del servicio (conectividad externa, factor de disponibilidad del servicio, capacidad soportada, etc.). Estos objetivos de nivel de servicio se habrán determinado previamente, a modo de parámetros cuantificables de manera objetiva, en el acuerdo de nivel de servicio¹⁷².

Veamos un ejemplo de este tipo de compensaciones¹⁷³:

170 Tomaremos como referencia la definición efectuada por GÓMEZ CALERO de la cláusula penal en el marco del Código de Comercio: "una estipulación contractual, de la que nace una obligación accesoria, que sirve a las partes para predeterminar las consecuencias del incumplimiento de un contrato mercantil mediante la fijación de una pena de carácter indemnizatorio contra el que no cumpliera, con lo cual -y dada la posibilidad de que la pena prescrita sea exigida por la parte perjudicada si el contrato no se cumple- se estimula al cumplimiento de dicho contrato y, en su caso, se sanciona al contratante que no cumple y se satisface a la parte perjudicada". GÓMEZ CALERO, Juan, *Contratos mercantiles con cláusula penal*, Madrid, 1983, pág. 59. De acuerdo con los conceptos de cláusula penal de los artículos 56 del Código de Comercio ("En el contrato mercantil en que se fijare pena de indemnización contra el que no lo cumpliera, la parte perjudicada podrá exigir el cumplimiento del contrato por los medios de derecho o la pena prescrita; pero utilizando una de estas dos acciones quedará extinguida la otra, a no mediar pacto en contrario") y 1152 a 1155 del Código Civil (art. 1252: "En las obligaciones con cláusula penal, la pena sustituirá a la indemnización de daños y al abono de intereses en caso de falta de cumplimiento, si otra cosa no se hubiere pactado"). En relación a las cláusulas penales en el *Outsourcing* informático, a modo de *performance credits*, ver APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática...*, *op. cit.*, pág. 94.

171 BRADSHAW, S; MILLARD, C; WALDEN, I, *Standard contracts...*, *op. cit.*, pág. 63.

172 Ver apartado "Descripción técnica de los acuerdos de nivel de servicio y sus parámetros: los objetivos de nivel de servicio", en este mismo capítulo.

173 "Should the Service Level fall below 99.9% for a given month, Microsoft will provide a Service Credit as noted in the chart below. Service Credit will be issued against the applicable month's Subscription Fee paid by Customer for the Service". (Traducción propia). Cláusula extractada del ANS del contrato de software como servicio) *Microsoft Dynamics CRM* [en línea]. Las cláusulas contractuales en español (<<https://port.crm.dynamics.com/portal/static/3082/tos.htm?lc=3082>>) contienen un enlace que dirige al SLA en inglés, (apartado 6.1). Disponible en: <<https://port.crm.dynamics.com/portal/static/1033/sla.htm>> [Fecha de consulta: 29 de noviembre de 2016].

CAPÍTULO SEXTO

"Si el acceso al servicio es inferior al factor de disponibilidad del 99,9% durante un determinado mes, [el proveedor] le proporcionará un crédito de servicio de acuerdo con la tabla siguiente: Si es inferior al 99,9 %, [recibirá un] crédito de servicio del 25%. Si es inferior al 99 %, [recibirá un] crédito de servicio del 50%. Si es inferior al 95 %, [recibirá un] crédito de servicio del 100%".

Como vemos, los créditos de servicio tienen características coincidentes con las cláusulas penales, en cuanto que son una declaración de voluntad tendente a predeterminar las consecuencias de un incumplimiento, tienen naturaleza convencional, se incorporan a un contrato mercantil del que dimana la obligación principal, y son fuente de una obligación accesoria¹⁷⁴.

Sin embargo, estas compensaciones o *service credits* no pueden considerarse, en nuestra opinión, verdaderas cláusulas penales. La naturaleza de la prestación que contemplan los créditos de servicio es una reducción del precio en futuras facturaciones del servicio, lo que implica para el prestador la pérdida de parte de los beneficios que el cliente le adeuda (o adeudará, al tratarse de facturaciones futuras aún no devengadas) por la prestación. Por tanto, esta "penalización", aunque tenga carácter pecuniario, no implicará para el proveedor la pérdida de activos económicos ya abonados, sino que, en su caso, dejará de percibir parte de los ingresos que se devengarán *a posteriori* del hecho causante del cumplimiento defectuoso¹⁷⁵. Ello fundamenta, a nuestro modo de ver, que los créditos de servicio, tal y como se conciben en los contratos de computación en la nube, no tengan una verdadera función punitiva o coactiva para el proveedor, porque no actúan como factor de

174 GÓMEZ CALERO, Juan, *Contratos mercantiles...*, op. cit., pág. 64.

175 Aunque los créditos de servicio están subeditados al incumplimiento de una obligación principal, cabe mencionar que no nos hallamos ante un incumplimiento absoluto de una obligación principal, sino ante un cumplimiento defectuoso o cumplimiento parcial de esa obligación, con lo cual creemos que quedará fuera del ámbito del concepto de cláusula penal del art. 56 del Código de Comercio, aunque este supuesto si aparece recogido en el régimen jurídico de obligación con cláusula penal del art. 1154 del Código Civil. En este art. 1154 se alude al supuesto de que "la obligación principal hubiera sido en parte o irregularmente cumplida". Sin embargo, el art. 56 del Código de Comercio no menciona ninguna modalidad de incumplimiento, y la pena viene fijada respecto de un incumplimiento absoluto, con lo cual, en casos de cumplimiento defectuoso, "el órgano judicial debe modificar equitativamente la cuantía de la pena para que no se produzca un enriquecimiento injusto". Así lo afirma GÓMEZ CALERO, al decir que "en la hipótesis del art. 56 del Código de Comercio, la pena viene fijada en contemplación del incumplimiento absoluto; así pues, la reclamación de la entera prestación penal por parte del acreedor puede dar origen a que este se enriquezca injustamente, (...)", y que, cuando un contrato mercantil con cláusula penal es defectuosamente cumplido, de acuerdo con los art. 56 del Código de Comercio y los art. 1152 y 1154 del Código Civil, "la parte perjudicada puede reclamar la pena; pero como la pena viene prevista para el incumplimiento absoluto y la obligación principal ha sido en parte o irregularmente cumplida, el órgano judicial debe modificar equitativamente su cuantía, y debe hacerlo de modo que el acreedor, entre la defectuosa prestación que ha obtenido y la cuota de pena que le es abonada, quede íntegramente satisfecho". GÓMEZ CALERO, Juan, *Contratos mercantiles...*, op. cit., págs. 137-156.

CAPÍTULO SEXTO

persuasión suficiente para forzar el cumplimiento, diferenciándose del concepto tradicional de cláusula penal¹⁷⁶.

Igualmente, debido al escaso contenido económico que comporta para el proveedor la satisfacción al cliente de un crédito de servicio, tampoco consideramos cumplida la función compensatoria de la cláusula penal, puesto que en ningún modo se valoran ni se toman como referencia los potenciales daños que hubiere podido acarrear en la actividad empresarial del cliente la interrupción del servicio o la imposibilidad de acceso a los datos migrados¹⁷⁷. Así, con los créditos de servicio no se pretende ofrecer al cliente un "equivalente pecuniario" al cumplimiento de la obligación, como método de resarcimiento.

Otra distinción remarcable entre los créditos de servicio y las cláusulas penales reside en la reclamación de los créditos. Mientras que, con la cláusula penal, es el perjudicado quien exige la reclamación de la pena, la configuración de estos créditos de servicio en los contratos hace que sea el proveedor quien decida si esa compensación se hace efectiva o no, posibilitando incluso liberarse de otorgar los créditos de servicio al cliente¹⁷⁸.

Coincidimos, por tanto, con la opinión del grupo de expertos de la *Cloud Computing Strategy*, en que estos créditos de servicio no operarían como cláusulas penales, puesto que estos créditos no permiten compensar con precisión las pérdidas reales¹⁷⁹. Los mismos expertos definen estos créditos de servicio como un mecanismo

176 En palabras de GÓMEZ CALERO, "esta otra prestación [aquella predeterminada por la cláusula penal] habrá de ser más gravosa que el cumplimiento mismo", con lo cual la cláusula penal, por definición, debe ser "lo suficientemente onerosa como para mover al cumplimiento" y servir "para sancionar al incumplidor y para satisfacer al perjudicado". GÓMEZ CALERO, Juan, *Contratos mercantiles...*, op. cit., pág. 58. En el mismo sentido, DÍEZ-PICAZO, Luis, "Cláusula penal y resolución del contrato", *Libro-Homenaje al profesor Amorós Guardiola*, Madrid, 2006, pág. 387.

177 Afirma GÓMEZ CALERO, respecto de la cláusula penal en el ámbito civil, que "puede tener un efecto valorativo, en cuanto la cláusula sirve para evaluar de antemano el importe de los daños y perjuicios que se pueden atribuir al incumplimiento o cumplimiento defectuoso o tardío de la obligación principal". GÓMEZ CALERO, Juan, *Contratos mercantiles...*, op. cit., pág. 90

178 Veamos un ejemplo de acuerdo de nivel de servicio en el cual queda patente la facultad del proveedor de decidir si concede o no los descuentos en concepto de créditos de servicio: "Si no logramos ni mantenemos los niveles de servicio para cada servicio tal como se describe en el presente SLA [o Acuerdo de Nivel de Servicio], el cliente puede ser elegible para recibir un crédito respecto de una parte de los precios de servicio mensuales". Acuerdo de nivel de servicio para servicios en la nube *Azure*, del proveedor Microsoft [en línea]. Disponible en: <https://azure.microsoft.com/es-es/support/legal/sla/cloud-services/v1_0/>. [Fecha de consulta: 29 de diciembre de 2016].

179 Discussion Paper 9, págs. 13-14, del Grupo de Expertos en contratos de la *Cloud Computing Strategy*, <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 17 de mayo de 2017].

CAPÍTULO SEXTO

contractual que sirve para ajustar el precio cuando varía el nivel de servicio de acuerdo con lo acordado inicialmente. Por tanto, según su opinión, no será posible considerar un incumplimiento contractual la no consecución de tales objetivos de nivel de servicio asociados a créditos de compensación, puesto que el precio ya se ha ajustado previamente a tal cumplimiento defectuoso.

Sí reconocen los mismos expertos que se producirá un incumplimiento cuando, dándose los requisitos pactados, el proveedor no quiera aplicar las rebajas que implican los créditos de servicio para compensar al cliente. En relación a la reclamación del crédito de servicio por parte del cliente, aunque de entrada se establezca una compensación en relación a la falta del deber de diligencia del proveedor, en las mismas cláusulas suelen incluirse requisitos que deben observarse para su reclamación, por ejemplo, plazos de aportación de información sobre el incidente que motiva la compensación, con lo cual no operan de forma automática, como sí sucede con la cláusula penal tradicional¹⁸⁰.

De igual manera, deben tenerse en cuenta las exclusiones que pueda hacer el proveedor en relación a factores que queden fuera del cómputo del objetivo de nivel de servicio. Por ejemplo, cuando se presentan compensaciones por falta de disponibilidad del servicio, generalmente no se tendrán en cuenta aquellos cortes de suministro de duración breve o intermitente, o las operaciones de mantenimiento de sistemas programadas con antelación¹⁸¹.

Se plantea entonces la cuestión de la comprobación, por parte del cliente, del cumplimiento o incumplimiento de estos niveles y de la correcta prestación del servicio. En relación a esta cuestión, el grupo de expertos de la *Cloud computing Strategy* se ha preguntado en qué forma deben comunicarse estas mediciones a los clientes (periodicidad, posibilidades de impugnación) y si debe o no existir

180 "Customer must provide sufficient evidence to support the Claim, by the end of the month following the month in which the Incident which is the subject of the Claim occurs (for example, Incident occurs on January 15th, Customer provides Notice on January 20th, Customer must provide sufficient evidence to support the Claim by February 28th)". (Traducción propia). Cláusula extractada del ANS del contrato de software como servicio *Microsoft Dynamics CRM*. Disponible en: <<https://port.crm.dynamics.com/portal/static/1033/sla.htm>>. [Fecha de consulta: 18 de mayo de 2017].

181 "Downtime does not include: "The period of time when the Service is not available as a result of Scheduled Downtime; or The following performance or availability issues that may affect the Service: (...) Intermittent periods of Downtime that are ten minutes or less in duration (...)". Cláusula extractada del ANS del contrato de SaaS (Software como Servicio) *Microsoft Dynamics CRM*. Disponible en: <<https://port.crm.dynamics.com/portal/static/1033/sla.htm>> [Fecha de consulta: 17 de mayo de 2017].

CAPÍTULO SEXTO

diferenciación entre la información que se aporte a empresas y a consumidores, o entre servicios gratuitos y servicios sujetos a contraprestación monetaria. Se presentan, además, otros problemas añadidos, como la cadena de proveedores que soporta el servicio o la falta de conocimientos técnicos y recursos financieros de la pequeña empresa para verificar la adecuación de la prestación a los objetivos de nivel de servicio acordados¹⁸².

Generalmente, los créditos de servicio se configuran como sustitutivos de indemnizaciones por daños, y como única compensación al alcance del cliente por incumplimientos de ciertos aspectos del acuerdo de nivel de servicio. Si bien son mecanismos que permiten ajustar el precio del servicio ante prestaciones defectuosas y que puede tener utilidad práctica cuando el incumplimiento defectuoso es meramente ocasional, también obstaculizan tanto la resolución del contrato ante incumplimientos defectuosos que tengan lugar de manera repetida durante la ejecución del servicio (pues obligan a la permanencia en el servicio para obtener su disfrute), como impiden la opción a las mencionadas indemnizaciones por daños y perjuicios¹⁸³. Por ello, no siempre resultan un mecanismo equitativo para el cliente, con lo cual los tribunales pueden, en cada caso, valorar su admisibilidad¹⁸⁴.

A diferencia de lo que sucede con los contratos que incluyen créditos de nivel de servicio como mecanismo para adaptar el precio a una eventual prestación parcialmente defectuosa, otros muchos contratos *cloud* excluyen expresamente la compensación por falta de disponibilidad del servicio u otras prestaciones defectuosas, al suscribirse un contrato con cláusulas que suponen la aceptación del servicio "tal y como está" y una consecuente redistribución de los riesgos de eventuales cumplimientos defectuosos entre las partes contractuales. Veremos con

182 *Discussion Paper 9*, pág. 1, del Grupo de Expertos en contratos de la *Cloud Computing Strategy*, <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 17 de diciembre de 2016].

183 *Discussion Paper 1*, pág. 3, del Grupo de Expertos en contratos de la *Cloud Computing Strategy*, <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 17 de diciembre de 2016].

184 Por su parte, la Unión Europea ha considerado, en trabajos que se llevan a cabo para la mejora de la protección del consumidor de contenidos digitales, que "los descuentos en el precio de futuros suministros de contenidos digitales, especialmente cuando son ofrecidos por los proveedores como una indemnización exclusiva por daños y perjuicios, no colocan necesariamente al consumidor en una posición lo más parecida posible a aquella en la que se encontraría si los contenidos digitales se hubieran suministrado debidamente y hubieran estado en conformidad con el contrato". Así lo afirma, en su motivo 44, la Exposición de Motivos de la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos del contrato de suministros de contenidos digitales, COM (2015) 634 final.

CAPÍTULO SEXTO

más detalle esta cuestión en el siguiente apartado.

4.- RESPONSABILIDAD DIRECTA DEL PROVEEDOR: LIMITACIONES Y EXONERACIONES. LA ACEPTACIÓN DE LOS SERVICIOS "TAL CUAL ESTÁN" Y "SEGÚN ESTÉN DISPONIBLES" ("AS IS" Y "AS AVAILABLE")

Los contratos que se tratarán en este apartado son contratos *cloud* cuyas condiciones generales incluyen limitaciones y exoneraciones de responsabilidad directa e indirecta. Entre ellos se encuentran los contratos que implican la aceptación por el cliente de los servicios "tal cual se prestan" ("as is" y "as available"). En este apartado analizaremos algunas de estas cláusulas y reflexionaremos sobre su consideración como abusivas para el pequeño empresario, por aplicación extensiva de la normativa de protección al consumidor¹⁸⁵.

4.1.- Las cláusulas limitativas y exonerativas de responsabilidad y distribución de riesgos entre las partes. Aceptación de los servicios "tal cual están"

La responsabilidad contractual entra en juego cuando una parte incumple (o cumple parcialmente) las obligaciones nacidas de un contrato, donde la parte que incumple deberá indemnizar a la parte perjudicada por tal incumplimiento (arts. 1101, 1106 y 1107 Código Civil¹⁸⁶). Cuando no exista ninguna relación contractual previa entre perjudicado y causante del daño, entrarán en juego el artículo 1902 y siguientes del Código Civil, que regulan la responsabilidad extracontractual¹⁸⁷.

En el contexto de contratación de servicios de nube pública que nos ocupa,

185 Respecto de los conceptos de empresario y consumidor como adherentes, nos remitimos al apartado "El destinatario de los servicios de la computación en la nube", en el capítulo "Elementos subjetivos del contrato de servicios de computación en la nube".

186 Art. 1101 del Código Civil: "Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas". Art. 1106 del Código Civil "La indemnización de daños y perjuicios comprende, no sólo el valor de la pérdida que hayan sufrido, sino también el de la ganancia que haya dejado de obtener el acreedor, salvo las disposiciones contenidas en los artículos siguientes". Art. 1107 del Código Civil "Únicamente se deben reparar los perjuicios que son consecuencia necesaria de su falta de cumplimiento y, salvo en caso de dolo, el deudor sólo responderá de los daños previstos o que se hayan podido prever al tiempo de constituirse la obligación".

187 REGLERO CAMPOS, Fernando, *Lecciones de responsabilidad civil*, Navarra, 2002, pág.43.

CAPÍTULO SEXTO

pueden existir cláusulas predispuestas por el proveedor *cloud* que modifiquen el régimen legal aplicable y den lugar a una nueva distribución de riesgos entre las partes, a través de las cuales el proveedor rehúse su responsabilidad. Si bien algunas de estas exoneraciones pueden ser justificables, como por ejemplo en aquellos casos en los cuales la adecuada recepción del servicio escape del control del proveedor (por ejemplo, debido a una deficiente conexión a Internet o a averías en los equipos), la validez de otras limitaciones de responsabilidad es más discutible, como sucede con las exclusiones de daños provocados directamente por una prestación defectuosa del servicio o por actuaciones negligentes del proveedor (interrupciones o errores del servicio, pérdidas de datos, problemas de confidencialidad, etc.)¹⁸⁸.

Los términos recogidos en condiciones generales en ocasiones implican la aceptación de los servicios de computación en la nube "tal cual están" o "según estén disponibles", utilizándose estas u otras expresiones similares (o sus traducciones en inglés "*as is*" y "*as available*" o expresiones similares)¹⁸⁹. Asumir el servicio tal y como

188 Encontramos una cláusula de exclusión de responsabilidad de validez discutible en las condiciones del proveedor "Box", que establece "Box presta los Servicios y ofrece el Sitio "tal cual" y "según están disponibles". En la medida que lo permita la ley aplicable y, a menos que se establezca expresamente en estas Condiciones, Box no realiza aseveraciones ni ofrece garantías ni condiciones de ningún tipo (y las niega todas específicamente) con respecto a los Servicios, ya sean expresas, implícitas, legales o de otra clase, incluidas, entre otras, las garantías de que los Servicios se prestarán de manera ininterrumpida, estarán exentos de errores o exentos de componentes dañinos, que el Contenido estará seguro y no se perderá o dañará, u otras garantías implícitas de calidad satisfactoria, idoneidad para un uso determinado, no infracción y cualquier garantía o condición que surja de la realización, el curso de la gestión o el uso comercial. Usted reconoce y acepta que utiliza los Servicios y el Sitio por decisión propia y bajo su propia cuenta y riesgo, y que es el único responsable de la pérdida de datos que se derive del envío o la descarga de dicho contenido". Condiciones del SaaS de almacenamiento del proveedor Box [en línea]. Disponibles en: <<https://www.box.com/legal/termservice/ES/>>. [Fecha de consulta: 6 de diciembre de 2016].

189 Igualmente, existen cláusulas en contratos *cloud* de adhesión que, aunque no coincidan con estos términos, de su lectura se extraen las mismas consecuencias legales: la limitación o exclusión de la responsabilidad directa por daños ocasionados por el servicio prestado, debido a una distribución de riesgos entre proveedor y adherente no siempre equitativa. Asimismo, las cláusulas de limitación o exclusión de responsabilidad no son exclusivas de los contratos de computación en la nube, sino que, como reconocía en su momento BELLO, son habituales en la mayoría de condiciones generales que predisponen los empresarios: "El estudio de las cláusulas de exclusión o reducción de responsabilidad en el ámbito de la protección de consumidores constituye uno de los aspectos esenciales del régimen de responsabilidad consagrado en la LCU, por varias razones: tanto por la inusitada frecuencia de tales declaraciones, habitualmente abusivas, cuánto por las carencias de su regulación en la LCU de 1984, carencias que vino a solventar, en parte, la LCGC, como, en fin, porque todo el régimen de responsabilidad previsto en los arts. 25 ss. LCU, de difícil interpretación armoniosa, carecería, en gran medida, de aplicación de aceptarse indiscriminadamente las declaraciones de exención de responsabilidad en los términos en que se suelen disponer por el empresario". BELLO JANEIRO, Domingo: "Cláusulas de exclusión o reducción de responsabilidad en la Ley General de Consumidores y Usuarios", *Anuario da Facultade de Dereito da Universidade da Coruña*, Nº 2, 1998, pág. 631.

CAPÍTULO SEXTO

se ofrece, en la práctica, supone renunciadas por parte del suscriptor del servicio a cualesquiera garantías que le correspondan por daños directos, entre las cuales se incluyen los daños que el suministro pueda producir a equipos, dispositivos, programas y datos del cliente, o pérdidas que pueda sufrir el negocio del pequeño empresario debido al mal funcionamiento del servicio *cloud* contratado.

La suscripción de estas cláusulas implica que el cliente está aceptando el servicio con todos sus defectos, tanto si estos defectos son perceptibles desde el momento de la contratación, como si se detectan o aparecen posteriormente. Desde nuestro punto de vista, deberá valorarse si estas cláusulas de exclusión de responsabilidad directa colisionan con el deber de diligencia exigible al proveedor del servicio respecto de las características y funcionalidades que integran la oferta comercial, y con su obligación legal de responder por daños ocasionados por mora, negligencia o dolo.

A diferencia de lo que sucede en otros ordenamientos, nuestra legislación no prevé expresamente criterios orientadores que ayuden al juez a ponderar la validez de estas limitaciones de responsabilidad en contratos suscritos por el pequeño empresario¹⁹⁰. Para realizar tal valoración, podrá acudir, en primer lugar, al artículo 8.1 de la Ley 7/1998 de 13 de abril, de Condiciones Generales de la Contratación, que establece que "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". En este caso,

190 A diferencia de nuestro ordenamiento, el ordenamiento jurídico inglés regula en la *Unfair Contract Terms Act* (UCTA) de 26 de octubre de 1977 las cláusulas de exclusión y limitación de la responsabilidad civil. Para determinar la validez de una cláusula que limite o excluya la responsabilidad, debe someterse al llamado test de razonabilidad, es decir, que las cláusulas sean equitativas, justas y razonables. Para ello, la propia Ley recoge en su anexo segundo (*schedule II*) los criterios que orientarán la estimación de la razonabilidad de la cláusula: el poder de negociación de las partes y las alternativas del cliente para satisfacer las necesidades que pretendía cubrir con el contrato, si el cliente recibió algún incentivo para acceder a la cláusula en cuestión, o si tuvo la ocasión de acudir a otros competidores en cuyo contrato no existiera una cláusula equivalente; si el cliente razonablemente podía esperar la inclusión de esta cláusula en el contrato, atendiendo a los usos del mercado; etc. A pesar de lo que pueda parecer, no obstante, cabe destacar que los tribunales ingleses son bastante restrictivos en cuanto a la interpretación de la razonabilidad de una cláusula predispuesta suscrita por un empresario. Para contratos suscritos por consumidores, el ordenamiento inglés cuenta con una regulación específica: la *Unfair Terms in Consumer Contracts Regulations*, aprobada el 14 de diciembre de 1994 con el fin de transponer la Directiva 93/13/CE sobre cláusulas abusivas, y que fue modificada en 1999, que, en lugar de someter a las cláusulas al test de razonabilidad, tiene en consideración la buena fe. Para un análisis más detallado, nos remitimos a MATO PACÍN, Natalia, "El control de contenido en la contratación mediante condiciones generales entre empresarios en el Derecho comparado y europeo", *Cuadernos de Derecho Transnacional*, 2015, Vol. 7, núm. 2, págs. 216 a 282.

CAPÍTULO SEXTO

podría entenderse su nulidad en contratos suscritos por pequeños empresarios, puesto que, como adherente, se le impide reclamar en aquellos casos en los cuales el proveedor *cloud* infrinja su deber de diligencia o preste un servicio defectuoso, dejándole sin posibilidad de interponer acción que le permita algún tipo de resarcimiento por daños y perjuicios sufridos, a lo cual tienen derecho de acuerdo con el artículo 1101 del Código Civil¹⁹¹.

Según nuestro criterio, en algunas contrataciones realizadas por pequeños empresarios podría aplicarse extensivamente la normativa de protección al consumidor¹⁹². Concretamente, la Directiva 93/13/CE sobre las cláusulas abusivas en los contratos celebrados con los consumidores (artículo 3 y anexo 1, letra b) y los artículos 80 y 82 a 90 del TRLGDCU pueden servir para orientar el juicio sobre la validez de estas limitaciones de responsabilidad en contratos suscritos por pequeños empresarios¹⁹³. Nos detendremos sobre esta cuestión en posteriores apartados de este

191 Art. 1101 del Código Civil: "Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas".

192 En el *Discussion Paper on Unfair Terms in Cloud Computing Contracts*, pág. 9, del Grupo de Expertos en contratos de la *Cloud Computing Strategy*, se afirma que estas cláusulas, en contratos con consumidores, pueden considerarse abusivas de acuerdo con el punto b) del Anexo I de la Directiva sobre las cláusulas abusivas en los contratos celebrados con consumidores [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 9 de diciembre de 2016]. Para más detalle, 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 este mismo capítulo.

193 Artículo 3 de la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre cláusulas abusivas en los contratos celebrados con consumidores: "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. (...) y anexo 3 de la misma Directiva, letra b: "b) excluir o limitar de forma inadecuada los derechos legales del consumidor con respecto al profesional o a otra parte en caso de incumplimiento total o parcial, o de cumplimiento defectuoso de una cualquiera de las obligaciones contractuales por el profesional, incluida la posibilidad de compensar sus deudas respecto del profesional mediante créditos que ostente en contra de este último". Artículo 80 Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias: "1. 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 (...), 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(...) y c) Buena fe y justo equilibrio entre los derechos y obligaciones de las partes, lo que en todo

CAPÍTULO SEXTO

capítulo¹⁹⁴.

Respecto de contratos suscritos por consumidores (cuyo ámbito de protección pretendemos que se haga extensible en algunas ocasiones al pequeño empresario), el artículo 86.1 del TRLGSCU permite declarar la abusividad de las cláusulas a través de las cuales, en nuestro caso, el proveedor de servicios *cloud* limita o excluye la responsabilidad que se derive de una prestación defectuosa del servicio, y le exime del cumplimiento de su deber de diligencia profesional. Ello es así porque tales cláusulas pueden calificarse como limitadoras de los derechos básicos de consumidor y usuario, al privarle de las acciones y compensaciones que legalmente le corresponden, y, por tanto, serían nulas en contratos suscritos por aquellos¹⁹⁵.

En todo caso, ante una demanda del adherente, el juez deberá valorar si se han producido abusos por parte del proveedor que permitan considerar la validez de ciertas cláusulas predispuestas en el contrato que rige la relación jurídica entre proveedor y cliente. El empresario que pretende integrar los servicios *cloud* en su actividad empresarial tendrá mucho más difícil que un consumidor conseguir una indemnización por daños cuando ha aceptado la prestación del servicio "tal y como está" o con otras cláusulas exoneratorias similares¹⁹⁶, teniendo que acudir a la

caso excluye la utilización de cláusulas abusivas. 2. Cuando se ejerciten acciones individuales, en caso de duda sobre el sentido de una cláusula prevalecerá la interpretación más favorable al consumidor". Los artículos 82 a 90 se refieren a las cláusulas abusivas. Respecto de la abusividad de las cláusulas en general, nos remitimos a REGLERO CAMPOS, Fernando, *Lecciones de responsabilidad civil*, Navarra, 2002, pág. 44.

194 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 este mismo capítulo.

195 Artículo 86.1 del TRLGDCU: "En cualquier caso serán abusivas las cláusulas que limiten o priven al consumidor y usuario de los derechos reconocidos por normas dispositivas o imperativas y, en particular, aquellas estipulaciones que prevean: 1. La exclusión o limitación de forma inadecuada de los derechos legales del consumidor y usuario por incumplimiento total o parcial o cumplimiento defectuoso del empresario. En particular las cláusulas que modifiquen, en perjuicio del consumidor y usuario, las normas legales sobre conformidad con el contrato de los bienes o servicios puestos a su disposición o limiten el derecho del consumidor y usuario a la indemnización por los daños y perjuicios ocasionados por dicha falta de conformidad".

196 Puesto que queda excluido de la definición de consumidor que realiza la Directiva 2011/83/UE del Parlamento Europeo y del Consejo de 25 de octubre de 2011 sobre los derechos de los consumidores, en su Considerando 17 ("La definición de consumidor debe incluir a las personas físicas que actúan fuera de su actividad comercial, empresa, oficio o profesión. No obstante, en el caso de los contratos con doble finalidad, si el contrato se celebra con un objeto en parte relacionado y en parte no relacionado con la actividad comercial de la persona y el objeto comercial es tan limitado que no predomina en el contexto general del contrato, dicha persona deberá ser considerada como consumidor") y en su art. 2: ("toda persona física que, en contratos regulados por la presente Directiva, actúe con un propósito ajeno a su actividad comercial, empresa, oficio o profesión"). También quedan fuera de la definición efectuada por el art. 3 del TRLGDCU ("A efectos de esta norma y sin perjuicio de lo dispuesto expresamente en sus libros

CAPÍTULO SEXTO

aplicación de los artículos¹⁹⁷ 1255, 1256, 1258 y 1911 del Código Civil¹⁹⁸. Por ello, según nuestro criterio y cuando ciertas circunstancias le sitúen en una posición equiparable a la del consumidor, debería poder acudir a los tribunales con la pretensión de la declaración de la nulidad de tales cláusulas no negociables. Si bien el pequeño empresario no es literalmente, formalmente ni materialmente consumidor, sí puede encontrarse en una situación de indefensión similar.

Actualmente se están llevando a cabo mejoras en la legislación europea de protección al consumidor que permitirán garantizar la responsabilidad del proveedor por daños ocasionados en el *hardware* o *software* del usuario cuando los recursos suministrados por el proveedor de contenidos digitales (en cuyo concepto se incluye el proveedor de servicios *cloud*) sean defectuosos¹⁹⁹. Una vez que estas mejoras sean aplicables, podría igualmente plantearse ante los tribunales su aplicación extensiva a contratos suscritos por pequeños empresarios que se encuentren en una situación similar a la de un consumidor.

En todo caso, consideramos recomendable para el cliente empresario que

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".

197 Afirma BELLO que "en el ámbito contractual, han de ser estimadas nulas, en principio, todas las convenciones que supongan o impliquen la exoneración total de responsabilidad del deudor, no ya sólo en virtud de lo dispuesto en el art. 1911 CC ["Del cumplimiento de las obligaciones responde el deudor con sus todos sus bienes, presentes y futuros"] sino, más claramente, porque el art. 1256 del mismo cuerpo legal ["La validez y el cumplimiento de los contratos no puede dejarse en manos de uno de los contratantes"] prohíbe que quede al arbitrio de una de las partes cumplir o no cumplir sus obligaciones". El autor refuerza este argumento con las sentencias STS de 4 de julio de 1953 y la Sentencia de la Audiencia Provincial de Barcelona, Sección 16, de 15 de noviembre de 1990.

198 Art. 1255 del Código Civil: "Los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por convenientes, siempre que no sean contrarios a las leyes, a la moral y al orden público". 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".

199 Concretamente, el artículo 14 de 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, que establece: "El proveedor será responsable ante el consumidor por cualquier daño económico ocasionado al entorno digital del consumidor debido a una falta de conformidad con el contrato de los contenidos digitales o a un incumplimiento en el suministro de los mismos. La indemnización por daños y perjuicios pondrá al consumidor en una posición lo más similar posible a aquella en la que se encontraría si los contenidos digitales se hubieran suministrado debidamente y hubieran estado de conformidad con el contrato. 2.- Los Estados miembros establecerán las condiciones detalladas para el ejercicio del derecho a reclamar daños y perjuicios". Esta propuesta, aunque se restringe a aquellos daños causados en el software o hardware del consumidor provocados por un incumplimiento en el suministro o a una falta de conformidad de acuerdo con lo acordado, permite dar cobertura a la mayoría de perjuicios que el consumidor del servicio *cloud* pueda sufrir.

CAPÍTULO SEXTO

pretenda suscribir servicios *cloud* que conlleven cláusulas de aceptación del servicio "tal y como se presta" que, previamente a la contratación, proceda a la investigación sobre el funcionamiento y el rendimiento del producto, la reputación del proveedor, las experiencias de otros usuarios o el pacto con el proveedor de un período de prueba que permita resolver del contrato sin penalizaciones o costes elevados.

Igualmente, consideramos necesaria una actuación legislativa que permita extender el ámbito de la abusividad de ciertas cláusulas suscritas por pequeños empresarios, cuya posición de manifiesta indefensión es, en algunos extremos y respecto de la suscripción en línea de servicios de computación en la nube pública y otros servicios similares, comparable a la del consumidor²⁰⁰.

4.2.- Límites cuantitativos y temporales a las indemnizaciones por daños y perjuicios

Al igual que son habituales las cláusulas de limitación o exclusión de responsabilidades en las condiciones generales de servicios de computación en la nube (como las anteriores cláusulas "as is" o "as available"), tampoco resultan extrañas las condiciones generales que limitan las indemnizaciones que el proveedor debe abonar a cada cliente por daños y perjuicios ocasionados por el servicio prestado (por ejemplo, daños provocados por la falta de disponibilidad, pérdida de datos, problemas de seguridad, etc.). Los límites pueden afectar al montante económico y/o al plazo de ejercicio de acciones de resarcimiento.

Respecto del importe que integra el contenido de la indemnización, los artículos 1106 y 1107 del Código Civil establecen que la reparación debe comprender los daños materiales o económicos y morales surgidos como daño emergente y lucro cesante. Aun así, es habitual que, a través de cláusulas generales, el contrato restrinja el montante económico que pueda recibir cada cliente en caso de que nazca la obligación de indemnizar por el proveedor, con lo cual el cliente únicamente puede ser indemnizado hasta un importe máximo²⁰¹. Este importe normalmente se

200 Nos remitimos, para más detalle, al 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 este mismo capítulo.

201 Art. 1106 del Código Civil. "La indemnización de daños y perjuicios comprende, no sólo el valor de la pérdida que hayan sufrido, sino también el de la ganancia que haya dejado de obtener el acreedor, salvo las disposiciones contenidas en los artículos siguientes". Art. 1107 del Código Civil: "Los daños y perjuicios de que responde el deudor de buena fe son los previstos o que se hayan podido prever al tiempo de constituirse la obligación y que sean consecuencia necesaria de su falta de cumplimiento. En caso de dolo responderá el

CAPÍTULO SEXTO

corresponderá con el precio total abonado por el servicio durante un determinado período²⁰², siendo una práctica común en el sector *cloud* que el proveedor no acepte riesgos que sobrepasen la contraprestación abonada por el cliente durante un cierto periodo, por la prestación del servicio²⁰³. En estos casos, se produce una merma en el derecho del cliente a ser resarcido por el valor equivalente a los daños sufridos.

Otra limitación que afecta al montante de la indemnización del cliente es aquella que excluye la reparación, por parte del proveedor *cloud*, del lucro cesante o, en términos del artículo 1106 del Código Civil, "la ganancia que haya dejado de obtener el acreedor", entre los cuales pueden incluirse aquellos ingresos dejados de percibir por pérdidas de reputación del cliente derivadas de una negligente actuación del proveedor de computación en la nube²⁰⁴.

deudor de todos los que conocidamente se deriven de la falta de cumplimiento de la obligación".

202 Cláusula extractada del Acuerdo para Empresas del SaaS (Software como Servicio) *G-Suite* (antes llamado *Google Apps for Work*). "Limitación de responsabilidades. "(...) 13.2 Limitación del importe por responsabilidad. Por la presente, ninguna de las partes será responsable del pago de una cantidad superior a la que el cliente haya pagado a Google según lo estipulado en este acuerdo, durante los doce meses anteriores al evento que haya dado lugar a la responsabilidad (...)". A continuación, otra cláusula predispuesta por el proveedor de Software como Servicio (SaaS) de almacenamiento remoto *Box*: "Límite de responsabilidad: en la medida que lo permitan las leyes aplicables, la responsabilidad total de Box y de sus filiales, ejecutivos, empleados, agentes, proveedores u otorgantes de licencias derivada o relacionada con el contrato: a) por servicios para los que no se adeude un pago se limitará a ciento ochenta euros (180,00 €); y b) en todos los demás casos, se limitará a las tarifas totales que usted paga a Box por el uso específico de los servicios que dan lugar a la reclamación en los doce (12) meses anteriores al acontecimiento que generase en primer lugar la demanda en virtud del contrato. Para evitar cualquier duda, este límite de la responsabilidad no se aplicará a ningún cliente que sea consumidor". Términos y condiciones de los servicios *G-Suite* y *Box* [En línea]. Disponibles respectivamente en: <https://gsuite.google.com/intl/es/terms/2013/1/premier_terms.html> y <<https://www.box.com/legal/termservice/ES/>>, respectivamente. [Fecha de consulta: 12 de diciembre de 2016].

203 Así se reconoce por el Grupo de Expertos en contratos de la *Cloud Computing Strategy*, en su *Discussion Paper on Unfair Terms in Cloud Computing Contracts* [en línea], pág. 11. Disponible en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 9 de diciembre de 2016].

204 Cláusula extractada del Acuerdo para Empresas del software como servicio *GSuite* (antes llamado *Google Apps for Work*). "Limitación de responsabilidades. "13.1 Limitación de las responsabilidades indirectas. Según este acuerdo, ninguna de las partes será responsable de los ingresos perdidos ni de ningún daño indirecto, especial, imprevisto, derivado, ejemplar o punitivo, aunque la parte supiera o debiera haber sabido que dichos daños eran posibles e incluso si los daños directos no satisfacen una compensación". El proveedor de software como servicio de almacenamiento remoto *Box* realiza esta limitación para clientes empresariales: "Box no será responsable, ya sea por contrato, (...) por cuestiones derivadas o relacionadas con este contrato o el objeto que lo concierne por: (i) pérdida de beneficios o ingresos, (ii) daños o pérdida del negocio o de la reputación, (iii) pérdida de ahorros anticipados, (iv) daños o pérdida del fondo de comercio, (v) pérdida de uso o corrupción de software, datos o información; (vi) cualquier pérdida o daño indirecto, especial o emergente. A efectos de esta cláusula, el término "pérdida" incluye la pérdida parcial o reducción del valor, así como la pérdida completa o total". [En línea]. Disponibles respectivamente en:

CAPÍTULO SEXTO

Cuando estas condiciones generales de limitación del derecho a la indemnización son suscritas por consumidores, carecen de validez, de acuerdo con las leyes aplicables en materia de protección de los derechos del consumidor²⁰⁵. Por ello, el consumidor tendrá derecho a ser resarcido de acuerdo con lo establecido en el artículo 8 del TRLGDCU, recibiendo una indemnización por daños y reparándose los perjuicios (lucro cesante y daños morales) sufridos²⁰⁶.

En relación a los límites que reducen el plazo para reclamar, el plazo para interponer tales acciones, basadas en el 1902 del Código Civil, viene determinado en nuestro ordenamiento por el art. 1968 del Código Civil, y es de un año²⁰⁷. Si en contratos suscritos por consumidores se establece una cláusula con un período menor, esta cláusula es abusiva. En cambio, si la condición se suscribe por un pequeño empresario, esta renuncia se entiende aceptable de acuerdo con el principio de la autonomía de la voluntad y de su deber de diligencia profesional que le es exigible al contratar. Somos partidarios de que también debería tenerse en consideración por los tribunales la situación de desequilibrio entre las partes, la falta de justificación de la reducción de este plazo, la dependencia que pueda tener el pequeño empresario de la prestación del servicio y la imposibilidad de negociar el contrato a la hora de valorar la pertinencia de una cláusula que reduzca considerablemente el plazo para reclamar una indemnización.

En resumen, tales cláusulas limitativas de los derechos del cliente respecto de indemnizaciones y del ejercicio de acciones que le corresponden legalmente serán abusivas para clientes consumidores de acuerdo con la Directiva 93/13/CE (anexo 1, letras b y q) y con el art. 86 TRLGDCU²⁰⁸. Respecto de contratos suscritos por un

<https://gsuite.google.com/intl/es/terms/2013/1/premier_terms.html> y
<<https://www.box.com/legal/termservice/ES>>. [Fecha de consulta: 12 de diciembre de 2016].

205 En concreto, de acuerdo con los artículos 86 del Texto Refundido de la Ley General de Consumidores y Usuarios, y 8 de la Ley de Condiciones Generales de la Contratación. Asimismo, la validez de esta cláusula que establece límites a los importes económicos de la indemnización en contratos con consumidores puede verse condicionada por la aprobación de nuevas normas especialmente orientadas a servicios digitales, como sucede con el mencionado artículo 14 de la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales.

206 Art. 8 TRLGDCU: "Son derechos básicos de los consumidores y usuarios: (...) b) La protección de sus legítimos intereses económicos y sociales; en particular frente a las prácticas comerciales desleales y la inclusión de cláusulas abusivas en los contratos. c) La indemnización de los daños y la reparación de los perjuicios sufridos".

207 Art. 1968 Código Civil. "Prescriben por el transcurso de un año: (...) La acción para exigir la responsabilidad civil por injuria o calumnia, y por las obligaciones derivadas de la culpa o negligencia de que se trata en el artículo 1.902, desde que lo supo el agraviado".

208 Art. 86.1 TRLGDCU: "En cualquier caso serán abusivas las cláusulas que limiten o priven al

CAPÍTULO SEXTO

cliente pequeño empresario, como se ha dicho, somos partidarios de la interpretación extensiva de estas normas, al no ser negociables y suponer un desequilibrio injusto entre las partes²⁰⁹. En caso de que no se apliquen de manera extensiva estas cláusulas en contratos suscritos por pequeños empresarios, deberemos acudir a las normas generales sobre contratos, como establece el artículo 8 de la Ley sobre Condiciones Generales de Contratación²¹⁰.

Por último, cabe puntualizar que estas indemnizaciones (limitadas cuantitativa o temporalmente) pueden quedar desplazadas, en casos de falta de disponibilidad del servicio (u otros que puedan determinarse), por los créditos de servicio (o *service credits*) especialmente dedicados a compensar el cumplimiento defectuoso del servicio, ya que, como se ha afirmado anteriormente, estos créditos de servicio suponen la renuncia a acciones de compensación del cliente²¹¹.

4.3.- La responsabilidad del proveedor por actuaciones de los subproveedores

Forma parte de la arquitectura *cloud* la posibilidad de que diferentes proveedores proporcionen recursos entre una u otra capa, a modo de suministro en cadena hasta que el servicio se presenta ante el cliente final²¹². La dinámica del servicio y del mercado exige de los proveedores finales flexibilidad y rapidez para cambiar o combinar aprovisionamientos de recursos procedentes de capas subyacentes, porque la subcontratación permite a los proveedores la reducción de costes, la escalabilidad del servicio y la no monopolización del mercado por grandes

consumidor y usuario de los derechos reconocidos por normas dispositivas o imperativas y, en particular, aquellas estipulaciones que prevean: 1. La exclusión o limitación de forma inadecuada de los derechos legales del consumidor y usuario por incumplimiento total o parcial o cumplimiento defectuoso del empresario. En particular las cláusulas que modifiquen, en perjuicio del consumidor y usuario, las normas legales sobre conformidad con el contrato de los bienes o servicios puestos a su disposición o limiten el derecho del consumidor y usuario a la indemnización por los daños y perjuicios ocasionados por dicha falta de conformidad".

209 En cuanto a la potencial abusividad de esta limitación para pequeños empresarios, 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 este mismo capítulo.

210 Art. 8 LCGC. "1. 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".

211 Ver apartado "El cumplimiento defectuoso y la determinación de *service credits* como indemnización al cliente".

212 Ver capítulos "Concepto y características técnicas de la computación en la nube" y "Elementos subjetivos del contrato de servicios de computación en la nube".

CAPÍTULO SEXTO

proveedores internacionales²¹³.

En cuanto a posibles reclamaciones por daños ocasionados al cliente del servicio *cloud* principal, cuando tales daños se deriven de un evento de fuerza mayor o un caso fortuito imprevisible e inevitable que haya podido ocasionarse en el ámbito del subproveedor de servicios, no existe razón por la cual el proveedor principal deba responder ante el cliente, ni tampoco el subproveedor (art. 1105 Código Civil)²¹⁴.

En las cadenas de subcontratación de los proveedores de servicios de computación en la nube que subyacen bajo contratos suscritos por pequeños empresarios (generalmente proveedores de software como servicio), el riesgo de que el cliente reciba un suministro insatisfactorio de recursos no siempre proviene del proveedor principal, sino que en la mayoría de ocasiones las deficiencias tienen su origen en proveedores de capas subyacentes (es decir, en servicios subcontratados de plataforma o infraestructura)²¹⁵. En muchas de estas ocasiones, el cliente *cloud*-pequeño empresario desconocerá la existencia de subproveedores o los integrantes de esa cadena de subcontratas.

A nuestro parecer, el contrato de computación en la nube que suscriben cliente pequeño empresario y proveedor debería recoger los servicios que pueden ser (o se hallan) subcontratados y la distribución de responsabilidades entre proveedor principal y subproveedores, para evitar el rechazo de futuras reclamaciones de responsabilidad efectuadas por el cliente empresario respecto de actuaciones de los subproveedores. Por el momento, los proveedores no suelen facilitar previamente esta información en los contratos con sus clientes, sino que se decantan por efectuar amplias exclusiones de responsabilidades como las ejemplificadas en anteriores apartados.

El cliente *cloud* pequeño empresario debería averiguar cuál es la cobertura que le ofrece el proveedor principal ante tales eventos, como parte de su deber de diligencia profesional, ya que, al carecer de poder de negociación en los contratos de adhesión en línea, se ve privado de exigir al proveedor que prevea contractualmente

213 *Discussion Paper 8* sobre subcontratación en los servicios de computación en la nube, del Grupo de Expertos en contratos de la *Cloud Computing Strategy* [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 17 de diciembre de 2016].

214 Art. 1105 Código Civil: "Fuera de los casos expresamente mencionados en la ley, y de los en que así lo declare la obligación, nadie responderá de aquellos sucesos que no hubieran podido preverse o, que, previstos, fueran inevitables".

215 Para más información sobre las capas que integran la arquitectura en la nube, ver capítulo "Concepto y características técnicas de la computación en la nube".

CAPÍTULO SEXTO

mecanismos de reparación cuando el origen del fallo en el suministro es provocado por un subproveedor del servicio *cloud*. Podría darse la circunstancia de que el proveedor principal obtenga compensaciones o pueda reclamar responsabilidades frente al subproveedor, porque así se prevea en el contrato suscrito entre ambos, mientras, al cliente pequeño empresario se le priva de cualquier vía de reparación, debido a la configuración del contrato final predispuesto por el proveedor y no negociable que limita o excluye estas responsabilidades. Según nuestro criterio, aunque es comprensible que la prestación adecuada del servicio *cloud* al cliente pequeño empresario dependa en gran parte del desempeño del subproveedor, debido al diseño de la arquitectura de la computación en la nube, ello no habilita al proveedor a escudarse en esa falta de control para eximirse de cualquier compensación a su cliente.

Según nuestro ordenamiento jurídico, no existe acción directa a favor del cliente contra las empresas subcontratadas, sino que responderá por ellas la empresa principal, de acuerdo con los arts. 1902 y 1903 del Código Civil²¹⁶. Posteriormente, el proveedor final podrá reclamar al contratista causante de los daños que hubiera tenido que abonar a los perjudicados, amparándose en el art. 1904 del Código Civil²¹⁷.

Asimismo, en el ámbito europeo se está proponiendo que el proveedor de suministro de contenidos digitales se responsabilice ante el suscriptor por las actuaciones de subproveedores que integren la cadena de transacciones. Debido al ámbito material de la normativa en la cual se trabaja, concretamente, la Propuesta de Directiva de suministro de contenidos digitales, es posible que esta posibilidad únicamente llegue a operar en aquellos casos en los cuales el destinatario del suministro de contenidos sea un consumidor. En todo caso, será la legislación nacional quien determine las condiciones del ejercicio de este derecho, si se aprobase la legislación comunitaria que lo contiene²¹⁸.

216 Código Civil: art. 1902: "El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado", y 1903: "La obligación que impone el artículo anterior es exigible, no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder. (...) Lo son igualmente los dueños o directores de un establecimiento o empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones. (...) La responsabilidad de que trata este artículo cesará cuando las personas en él mencionadas prueben que emplearon toda la diligencia de un buen padre de familia para prevenir el daño".

217 Art. 1904 del Código Civil. "El que paga el daño causado por sus dependientes puede repetir de éstos lo que hubiese satisfecho".

218 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. Artículos 10 "El proveedor será responsable ante el consumidor por: a) cualquier incumplimiento en el suministro de contenidos digitales, b) cualquier falta de conformidad que exista en el momento de suministrar los

CAPÍTULO SEXTO

Cuando el cliente *cloud* actúe como consumidor, y en las condiciones generales que haya suscrito medie una cláusula de exención de responsabilidad del prestador final del servicio por daños causados por subproveedores, de acuerdo con el art. 82.4 TRLGDCU, esta cláusula podrá ser declarada abusiva por limitar su derecho a recibir una compensación²¹⁹. Cuando esta exención de responsabilidad haya sido aceptada por un cliente pequeño empresario, puede entenderse que ha renunciado expresamente a la acción compensatoria, renuncia que se presumirá válida por el poder de disposición de los propios intereses que le concede la autonomía de la voluntad privada (art. 1255 del Código Civil²²⁰)²²¹. En todo caso, deberá revisarse si ese pequeño empresario se encuentra en una posición de indefensión similar a la del consumidor.

Por último, cabe recordar que el nuevo Reglamento General de Protección de Datos establece que el responsable del tratamiento que haya tenido que indemnizar al titular de los datos personales perjudicado, puede repetir ante el encargado cuando el incumplimiento en materia de privacidad sea responsabilidad de este o de un subencargado contratado por este²²².

contenidos digitales, y c) cualquier falta de conformidad que tenga lugar durante un periodo de tiempo, cuando el contrato establezca que los contenidos digitales se suministrarán a lo largo de dicho periodo" y 17: "Cuando el proveedor sea responsable ante el consumidor del incumplimiento en el suministro de contenidos digitales o de una falta de conformidad con el contrato resultante de una acción u omisión de una persona anterior en la cadena de transacciones, el proveedor podrá emprender acciones contra la persona responsable en dicha cadena. La legislación nacional determinará quién es el responsable y las acciones y condiciones de ejercicio correspondientes".

219 Aunque existe, en el art. 86.2 del TRLGDCU, la declaración de abusividad de "las cláusulas que limiten o priven al consumidor y usuario de los derechos reconocidos por normas dispositivas o imperativas y, en particular, aquellas estipulaciones que prevean: 2.-La exclusión o limitación de la responsabilidad del empresario en el cumplimiento del contrato, por los daños o por la muerte o por las lesiones causadas al consumidor y usuario por una acción u omisión de aquél", observamos que, para aplicar este precepto, se exige que la renuncia afecte a daños ocasionados por acciones u omisiones del propio empresario. Sin embargo, en el caso que nos ocupa, la acción u omisión causante de los daños ha sido realizada por un tercero subcontratista. Por este motivo, nos remitimos a la determinación de la abusividad general del art. 82.4 y a su potencial aplicación extensiva en contratos suscritos por pequeños empresarios en situación de indefensión similar a la del consumidor: "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: (...) c) limiten los derechos del consumidor y usuario".

220 Art. 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".

221 Respecto de nuestra opinión sobre la consideración de esta cláusula como abusiva en ciertos contratos suscritos por pequeños empresarios, 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 este mismo capítulo.

222 Ver apartado "Responsabilidad por incumplimiento de obligaciones en materia de protección de datos", en el capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

CAPÍTULO SEXTO

4.4.- Breve reflexión relativa a la aplicación extensiva de las normas sobre cláusulas abusivas al pequeño empresario. Extensión al ámbito de la contratación de servicios de *Cloud Computing*

Como es sabido, en nuestro país la regulación de las cláusulas predispuestas aparece recogida principalmente por dos normas (sin perjuicio de otras normas sectoriales²²³): la Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación, y el Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de Consumidores y Usuarios y otras leyes complementarias (en adelante, TRLGDCU).

En capítulos anteriores nos hemos referido al concepto de consumidor, así como a los controles legales de incorporación y contenido de cláusulas que puedan ser perjudiciales para el suscriptor, al ser contrarias a la buena fe y/o suponer un desequilibrio importante en los derechos u obligaciones derivados del contrato²²⁴.

A continuación, nos centraremos en las cláusulas habitualmente incluidas en contratos de computación en la nube susceptibles de ser suscritas por el pequeño empresario que podrían resultar ineficaces de acuerdo con la Ley de Condiciones Generales de la Contratación²²⁵.

Asimismo, expondremos nuestra posición respecto de una eventual aplicación extensiva de la protección del consumidor, concretamente respecto de las cláusulas abusivas incorporadas en contratos de adhesión suscritos por pequeños empresarios, cuando tales cláusulas supongan una merma en los derechos del pequeño empresario que, por verse necesitado de incorporar el servicio *cloud* a su actividad profesional (ya sea por razones de eficacia en la operativa, ya sea por cuestiones de ahorro de costes y mejora de su competitividad), se ve obligado a aceptar porque carece de

223 Por ejemplo, la Ley 50/1980 del Contrato de Seguro.

224 Ver apartado dedicado al consumidor como destinatario de servicios *cloud*, en el capítulo "Elementos subjetivos del contrato de servicios de computación en la nube".

225 La propia Ley de Condiciones Generales de la Contratación (art. 5.5 y 7 b) establece el mecanismo del control de incorporación para adherentes empresarios, pero reserva el control de contenidos al adherente consumidor. Ambos controles tienen finalidades distintas: el primero persigue que el adherente comprenda la carga económica y jurídica del contrato; el segundo, el equilibrio entre las prestaciones de las partes. SÁNCHEZ MARTÍN, Carlos, "La contratación bajo condiciones generales de la contratación frente a la contratación por negociación. Sus mecanismos específicos de control: abusividad y transparencia. La eficacia contractual resultante tras la declaración de abusividad", *Diario La Ley*, núm. 8333, Sección Tribuna, 16 de junio de 2014, pág. 2. Sin embargo, la verdadera necesidad de protección del pequeño empresario adherente de contratos de computación en la nube se halla, a nuestro parecer, en el contenido de las cláusulas y sus efectos sobre los intereses del adherente empresario.

CAPÍTULO SEXTO

posibilidad alguna de negociar tales cláusulas y se encuentra en posición de inferioridad contractual respecto del proveedor de los servicios *cloud*.

4.4.1.- Cláusulas abusivas y contratos de computación en la nube

Una de las cuestiones que cabría plantearse es si existen elementos específicos en la naturaleza del contrato de computación en la nube que puedan motivar este desequilibrio contractual entre proveedor y adherente, especialmente en aquellos contratos sin contraprestación dineraria o de bajo coste. Desde nuestra perspectiva, la contraprestación que realiza el cliente (sea este pequeño empresario o consumidor) a cambio de utilizar el servicio es irrelevante en cuanto a la introducción en el contrato de cláusulas abusivas, puesto que es el proveedor quien, tras realizar los respectivos estudios de mercado, decide libremente establecer un precio por sus servicios u otras contraprestaciones no dinerarias pero que igualmente poseen valor económico²²⁶.

En opinión del grupo de expertos de la *Cloud Computing Strategy*, en la contratación de servicios de nube pública con condiciones generales existen varias cláusulas que suponen una situación de desequilibrio para el cliente (pequeño empresario o consumidor)²²⁷. Concretamente, según el grupo de expertos, el punto de mira recae en un conjunto de cláusulas predisuestas con ciertos contenidos,

226 Ver apartado dedicado a la onerosidad en el contrato de computación en la nube, en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

227 Así lo afirma el grupo de expertos en contratación de la *Cloud Computing Strategy*, en su *Discussion Paper: Unfair Terms in Cloud Computing Contracts* (pág. 1), y en su síntesis de 5 y 6 de marzo de 2014 (pág.6). [En línea]. Disponibles respectivamente en: <http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_unfair_contract_terms_en.pdf>, y <http://ec.europa.eu/justice/contract/files/expert_groups/5_6_march_meeting_synthesis_final_en.pdf> [Fecha de consulta: 15 de diciembre de 2016]. Además afirman, como también se ha puesto de relieve en este trabajo, que cuando estos contratos sean suscritos por consumidores, tales condiciones generales son susceptibles de ser consideradas cláusulas abusivas. Estas observaciones sobre la abusividad de cláusulas habituales en contratos de servicios de computación en la nube son predicables de otros contratos de adquisición de bienes o servicios en línea que también pueden incluirlas, y también constatan que estas cláusulas son más habituales en los contratos sin contraprestación dineraria o de bajo coste predisuestos por proveedores radicados fuera de las fronteras comunitarias. Algunas de las afirmaciones realizadas por el Grupo de Expertos se sustentan en un informe sobre cláusulas abusivas en contratos de *Cloud Computing* con consumidores, elaborado por la Organización de Consumidores Europeos BEUC (*Bureau Européen des Unions de Consommateurs*). [En línea]. Disponible en: <http://www.beuc.eu/publications/beuc-x-2014-034_are_ec_expert_group_on_cloud_computing_contracts.pdf>. [Fecha de consulta: 15 de diciembre de 2016].

CAPÍTULO SEXTO

especialmente: aquellas que determinan ciertas exclusiones y limitaciones de responsabilidad; las que establecen la facultad unilateral del proveedor para modificar, suspender o extinguir unilateralmente la relación contractual, o aquellas que establecen unos plazos de notificación por rescisión del contrato más amplio para el cliente que para el proveedor; las que condicionan o limitan el ejercicio de los derechos para ejercitar acciones por incumplimiento o reclamaciones por daños (plazos reducidos para interponer reclamaciones, renunciaciones a sistemas de compensación, etc.); y aquellas que establecen límites a la propiedad de los contenidos migrados por el cliente.

4.4.2.- Cláusulas abusivas y pequeños empresarios

La contratación en masa se ha reconocido por la jurisprudencia como un modo de contratar diferenciado de la tradicional contratación por negociación regulada en el Código Civil²²⁸. A medida que se generaliza la suscripción de condiciones generales en la contratación en línea, y puesto que el pequeño empresario se ve obligado a participar cada vez más de los servicios informáticos prestados a través de Internet para mantener su competitividad, se va haciendo más patente la necesidad de protegerle de aquellas situaciones en las que pueda sufrir abusos o se vea injustificadamente perjudicado²²⁹.

228 Así se reconoce en las sentencias del Tribunal Supremo de 18 de junio de 2012, Sala Primera (res. 406/2012); de 9 de mayo de 2013, Sala Primera (res. 241/2013); de 20 de marzo de 2014, Sala Primera (res. 149/2014) y de 7 de abril de 2014, Sala Primera (res. 166/2014). SÁNCHEZ MARTÍN, Carlos, "La contratación bajo condiciones generales...", *op. cit.*, pág. 2.

229 En este sentido nos planteamos, al igual que otros autores, si existen razones que justifiquen regulaciones diferentes para el consumidor y aquel pequeño empresario que se encuentre en una situación de desequilibrio contractual similar. Concretamente, ALFARO se manifiesta en favor de un control del contenido de condiciones generales suscritas entre empresarios afirmando que "la noción de consumidor es un criterio inadecuado para delimitar el ámbito de aplicación de la legislación de control de las condiciones generales. La misma debe aplicarse con independencia de quienes sean los sujetos que contraten", y que "Si bien cabe admitir que las necesidades de protección sean mayores en el caso de los consumidores, no parece que ello justifique en modo alguno que los empresarios no sean protegidos frente al empleo de condiciones generales. (...), el predisponente, al configurar el contenido del contrato, actúa sin el control del mercado, lo que le permite establecer condiciones ventajosas para él mismo". ALFARO ÁGUILA-REAL, Jesús, *Las condiciones generales de la contratación. Estudio de las disposiciones generales*, Madrid, 1991, págs. 474 y 176. Por otra parte, algunos trabajos cuestionan los principales motivos que suelen fundamentar esta distinción, existente en la Directiva 2011/83/UE tales como que es económicamente más débil, que está insuficientemente informado, que puede carecer de alternativas a contratar tales condiciones, o que con la equiparación de consumidores y ciertos pequeños empresarios y profesionales pueda reducirse la protección del consumidor, al parecer este menos vulnerable. Así, quedaría en manos de los legisladores nacionales la eventual protección del pequeño empresario adherente. HESSELINK, M. W., "Towards a sharp distinction between b2b and b2c? On consumer, commercial and general law after the Consumer Rights Directive", *European Review of Private Law*, núm. 1, 2010, págs. 92 y ss.

CAPÍTULO SEXTO

En el ámbito europeo, se está reflejando esta tendencia, y aunque de momento no llegue a consolidarse en forma de normativa²³⁰, la Estrategia de la Comisión Europea para un Mercado Único Digital ha identificado la necesidad de reforzar la posición contractual del pequeño y mediano empresario frente a grandes proveedores de contenidos digitales²³¹. De manera similar lo había contemplado el

230 El artículo 86 de la malograda Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a una norma común de compraventa europea permitía considerar abusivas ciertas cláusulas suscritas en contratos de adhesión entre empresarios, aunque establecía diferencias entre el concepto de abusividad en relación al aplicado en contratos suscritos por consumidores, restringiendo su virtualidad únicamente para aquellos contratos de adhesión entre empresas que se aparten manifiestamente de las "prácticas comerciales habituales" y que contradigan la buena fe contractual. Este artículo parecía reconocer que el hecho de que una práctica sea utilizada mayormente en el mercado, como sucede con muchas de las cláusulas potencialmente abusivas incluidas en contratos *cloud*, no tiene porqué significar que sea equitativa. Esta Propuesta de Reglamento europeo no prosperó, y se substituyó por las Propuestas de Directivas COM(2015) 634 final y COM(2015) 635 final, relativas respectivamente a determinados aspectos de los contratos de suministro de contenidos digitales y a determinados aspectos de los contratos de compraventa en línea y otras ventas a distancia de bienes, aunque ambas restringen su ámbito a contratos suscritos con consumidores. Artículo 86 de la Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a una norma común de compraventa europea (CESL): "Significado del término «abusivo» en los contratos entre comerciantes: 1. Una cláusula incluida en un contrato celebrado entre comerciantes será abusiva a efectos de la presente sección solo si: a) forma parte de cláusulas no negociadas individualmente a tenor del artículo 7; y b) resulta de tal naturaleza que su aplicación se aparta manifiestamente de las prácticas comerciales habituales, en contra de las exigencias de la buena fe contractual. 2. A efectos de la presente sección, a la hora de evaluar si una cláusula contractual resulta abusiva, deberá atenderse a: a) la naturaleza de lo que se proporciona a través del contrato; b) las circunstancias concurrentes en el momento en que se celebró; c) el resto de las cláusulas contractuales; y d) las cláusulas de cualquier otro contrato del cual dependa".

231 Las Propuestas de Directivas sobre suministro de contenidos digitales y compraventa de bienes en línea anteriormente mencionadas reconocen la existencia de problemas en las relaciones contractuales entre PYME y proveedores en línea. Así, la Propuesta de Directiva COM(2015) 634 final afirma, al detallar el contenido del artículo 3, que "La Directiva solo cubre las transacciones entre empresas y consumidores. Los problemas relacionados con el derecho contractual en las relaciones entre empresas, especialmente en relación con las necesidades específicas de las PYME, han sido identificados en la Estrategia para un Mercado Único Digital, y serán analizados en el contexto de otras acciones anunciadas en la Estrategia". Por su parte, la Propuesta 635 (2015) final, al exponer el resumen de los resultados del proceso de consulta a las partes interesadas, informa de que "teniendo en cuenta las diferentes características de los contratos B2B y B2C y las posibles fricciones con los instrumentos legales ya existentes, las organizaciones de consumidores no respaldan la inclusión de los contratos B2B en el ámbito de esta propuesta", aunque "la gran mayoría de asociaciones de las profesiones del ámbito jurídico estarían a favor de normas armonizadas de la Unión, y del mismo régimen para los contratos B2C y B2B", y "La gran mayoría de Estados miembros que han contestado solo apoyan la inclusión de contratos B2C". En la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una Estrategia para el Mercado Único Digital de Europa, COM(2015) 192 final, se reconoce la necesidad de eliminar los obstáculos en las transacciones transfronterizas en línea y la necesidad de definir un marco de comercio electrónico adecuado y que impida discriminaciones injustas contra consumidores y empresas que intentan acceder a contenidos o comprar bienes y servicios en línea. (punto 2 de la comunicación). En el apartado titulado *Un*

CAPÍTULO SEXTO

Marco Común de Referencia (*Draft Common Frame of Reference*), en su Principio 46 y en su artículo II-9:405, sobre el concepto de abusividad en contratos entre empresarios²³². Así, se enfatiza que el concepto de abusividad entre empresarios se entenderá en aquellos casos en los que una cláusula de adhesión sea contraria a las buenas prácticas comerciales y sea contraria a la buena fe contractual. Por contra, en el artículo II-9:403 se establece que se entenderá que una cláusula suscrita por consumidores es abusiva cuando, además de ser contraria a la buena fe contractual, implique desventajas significativas para el consumidor.

A nuestro modo de ver, uno de los fundamentos de la distinción entre cláusulas eventualmente abusivas suscritas por el pequeño empresario y aquellas suscritas por el consumidor es que al primero, al actuar en el marco de una actividad empresarial, se le presume el deber de diligencia profesional en su ejercicio mercantil, y, por ende, la valoración de la pertinencia de contratar ciertos servicios a través de cláusulas no negociables. Sin embargo, al hallarnos ante prácticas contractuales desproporcionadas, injustas y tan extendidas que pueden llegar a considerarse comunes en la comercialización de los servicios de computación en la

marco regulador adecuado para los fines previstos para las plataformas y los intermediarios. Papel de las plataformas en línea, la Comisión afirma que "las plataformas en línea (por ejemplo, los motores de búsqueda, las redes sociales, las plataformas de comercio electrónico, las tiendas de aplicaciones, los sitios web de comparación de precios) están desempeñando un papel cada vez más central en la vida económica y social: permiten a los consumidores obtener información en línea y a las empresas aprovechar las ventajas del comercio electrónico. (...). Esto ha dado lugar a una serie de preocupaciones sobre el creciente poder de mercado de algunas plataformas. Entre ellas figuran la falta de transparencia sobre la manera en que utilizan la información que obtienen, su fuerte poder de negociación frente al de sus clientes, que puede reflejarse en sus términos y condiciones (especialmente para las PYME), la promoción de sus propios servicios en detrimento de los competidores y la falta de transparencia de las políticas de precios, o restricciones en la fijación de precios y condiciones de venta". Sin embargo, la Comisión no se compromete en esta Estrategia, al menos por el momento, y a pesar de lo indicado en las mencionadas Propuestas de Directiva, a ninguna actividad que haga prever una pronta evaluación de la situación contractual de PYME que contratan servicios de suministro de contenidos en línea y de su situación de discriminación injusta. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una Estrategia para el Mercado Único Digital de Europa, COM (2015) 192 final [en línea]. Disponible en: <<http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0192&from=EN>>. [Fecha de consulta: 15 de diciembre de 2016].

232 Marco Común de Referencia. Principio 46: "Protecting the vulnerable. (...) People presented with standard terms prepared by the other party are also in a vulnerable position in practice, whether or not they are consumers, and there are rules in the DCFR to protect them". Artículo II-9:405: "Meaning of "unfair" in contracts between businesses. A term in a contract between businesses is unfair for the purposes of this Section only if it is a term forming part of standard terms supplied by one party and of such a nature that its use grossly deviates from good commercial practice, contrary to good faith and fair dealing". Artículo II-9:403: "In a contract between a business and a consumer, a term [which has not been individually negotiated] is unfair for the purposes of this Section if it is supplied by the business and if it significantly disadvantages the consumer, contrary to good faith and fair dealing".

CAPÍTULO SEXTO

nube, consideramos necesarias mejoras legales que protejan al pequeño empresario de abusos de proveedores que tienen lugar a través de contratos de adhesión, y que permitan un mejor reflejo legal del principio de buena fe contractual entre empresarios.

En el ámbito internacional, existen algunos Estados miembros que han reforzado el nivel de protección de pequeños y medianos empresarios, como Alemania, Portugal u Holanda, que contemplan expresamente un control de contenido en contratos suscritos por empresarios a través de condiciones generales, fundamentados en la falta de negociación, la dependencia del adherente y el desconocimiento real del clausulado por falta de asesoramiento o experiencia. Debe destacarse que, en estos ordenamientos, el tratamiento de los contratos entre empresarios se diferencia del de los consumidores, introduciendo criterios relacionados con los usos comerciales, o las dimensiones de la empresa adherente y su efectivo poder de negociación, tal y como afirman ciertos autores²³³. En nuestra opinión, una regulación de la contratación entre empresarios que restrinja ciertas prácticas perjudiciales para empresas suscriptoras y que se base en los criterios orientadores anteriormente mencionados (imposibilidad de negociación, necesidad del servicio, falta de experiencia o de conocimientos técnicos, desequilibrio entre las partes contractuales, etc.) sería deseable no solo en nuestro país, sino en el ámbito europeo.

En España, los contratos de adhesión entre empresas se rigen por la legislación específica (es decir, la Ley de Condiciones Generales de Contratación, en lo que resulte de aplicación, o, en la legislación especial de otros contratos, como el contrato de seguro) y, en su defecto, por lo dispuesto por el Código de Comercio y, de manera supletoria, por el Código Civil.

Así, se distingue por la Ley sobre Condiciones Generales de la Contratación (en adelante, también LCGC) entre adherente consumidor y no consumidor, aunque la posición jurídica del pequeño empresario adherente pueda asemejarse a la situación de desequilibrio contractual del consumidor, como sucede en muchos contratos en línea con cláusulas predispuestas y no negociables²³⁴.

233 Para un estudio comparativo más detallado, nos remitimos a MATO PACÍN, Natalia, "El control de contenido en la contratación mediante condiciones generales entre empresarios en el Derecho comparado y europeo", *Cuadernos de Derecho Transnacional*, Octubre 2015, Vol. 7, Nº 2, págs. 216-282; y a ALBIEZ DOHRMAN, Klaus Jochen, *La protección jurídica de los empresarios en la contratación de condiciones generales*, 1ª edición, Navarra, 2009, págs. 19 a 114.

234 Se considera adherente, conforme al art. 2 de la Ley sobre Condiciones Generales de

CAPÍTULO SEXTO

La norma prevé para el empresario adherente un control de ciertos requisitos que deben cumplir las cláusulas para entenderse incorporadas en las condiciones generales: el denominado control de inclusión o de incorporación²³⁵. El control de incorporación de las condiciones generales es aquel conjunto de medidas legales dirigido a que el adherente pueda conocer la existencia de las cláusulas predisuestas y entender su alcance, y que sean transparentes, y para ello serán relevantes aspectos como tamaño de la letra, el idioma de las cláusulas, la visibilidad del documento (documento electrónico o sitio web, en el caso de la contratación *cloud*) que las contiene, la claridad de la redacción, etc.

Por otra parte, existe el control de contenido, que determinará cuándo una norma es abusiva, aunque haya sido conocida y suscrita por el adherente. En el supuesto del adherente empresario no se realiza un control del contenido de las cláusulas predisuestas²³⁶. Ello es así porque, de acuerdo con el nuestro

Contratación, a aquella persona que concluye un contrato por medio de condiciones generales predisuestas por el otro contratante, lo que incluye a contratantes consumidores y no consumidores. Este sujeto apenas cuenta con libertad negocial, puesto que su única capacidad de decisión suele residir en la aceptación o no de las condiciones propuestas, es decir, en la aceptación o no aceptación del contrato. Esta condición le posiciona como parte débil del contrato. Su contraparte, el predisponente, es la persona física o jurídica que utiliza cláusulas pre-redactadas elaboradas con la finalidad de incluirse en múltiples contratos, en el ejercicio de su actividad profesional o empresarial (arts. 1 y 2 LCGC). La posición débil en el contrato se debe a un desequilibrio jurídico entre las partes, respaldado a su vez por un desequilibrio económico entre predisponente y adherente consumidor o profesional-pequeño empresario. BADENAS CARPIO, Juan, "Ámbito Subjetivo de la Ley de Condiciones Generales de la Contratación", *Comentarios a la Ley de Condiciones Generales de la Contratación* (Coord. Rodrigo Bercovitz Rodríguez-Cano), 1ª edición, Navarra, 2000, págs. 67, 86, 89.

235 PARDÓ GATO, José Ricardo, *Las cláusulas abusivas en contratos de adhesión*, 1ª Edición, Madrid, 2004, págs. 138-140, 182-184; CLAVERÍA GOSÁLBEZ, Luís Humberto; *Condiciones Generales y cláusulas contractuales impuestas*, 1ª Edición, Barcelona, 2008, págs. 36-37. LLODRÁ GRIMALT; Francisca; *El contrato celebrado bajo condiciones generales*, Valencia, 1ª edición, 2002, págs. 259-268, 346-347; ALFARO ÁGUILA-REAL, Jesús, *Las condiciones generales de la contratación. Estudio de las disposiciones generales*, Madrid, 1991, 482 págs.; y ALFARO ÁGUILA-REAL, Jesús, "Cláusulas abusivas, cláusulas predisuestas y condiciones generales", *Anuario Jurídico de La Rioja*, núm. 4, 1998, págs. 53-70.

236 En opinión de algunos autores, este control de contenidos debería ser diferente e independiente del control efectuado a las condiciones generales suscritas por consumidores, por varias razones. Una de ellas es que, a diferencia de lo que ocurre el mandato del ordenamiento en relación a la protección de los consumidores, el Estado debería reducir en la medida de lo posible su intervención en las relaciones interempresariales, para no entorpecer la autonomía contractual de las partes, puesto que el empresario tiene sus propias reglas negociales (marcadas por el Derecho mercantil), y sus propios mecanismos de defensa para soportar cláusulas contrarias a sus intereses. Por tanto, puede ser perjudicial para el tráfico jurídico equiparar por defecto a cualquier empresa con el consumidor. Lo ideal sería, según estos autores, una solución menos intensa, ponderando múltiples variables, como la efectiva debilidad de los adherentes (aquellos que sean

CAPÍTULO SEXTO

ordenamiento jurídico, solo puede declararse la nulidad de una cláusula general que obre en un contrato entre empresarios cuando contradiga el derecho imperativo, la moral y el orden público (art. 1255 del Código Civil), pero no por su abusividad, ya que este régimen estaría reservado a los contratos suscritos por consumidores²³⁷. Lo anterior no es óbice, sin embargo, para que se le aplique la regla *in dubio, contra proferentem*, en cuanto a la interpretación de cláusulas poco transparentes en contratos suscritos por el pequeño empresario (art. 1288 del Código Civil)²³⁸.

Se apuntan por algunos autores otras alternativas al control de contenido de las condiciones generales, como un control a través del Derecho de la competencia (y la imposición de límites que eviten el abuso de posición dominante) o recomendaciones y dictámenes sobre la validez de condiciones de contratación por distintas instituciones y organismos, a modo de buenas prácticas contractuales²³⁹.

profesionales independientes o empresas de pequeña envergadura o volumen de negocio no deben ser equiparados a grandes empresas, puesto que estas últimas pueden tolerar o compensar la introducción en los contratos de cláusulas gravosas mediante otras condiciones o pactos). La sentencia del Tribunal Supremo de 26 de abril de 2004, consideró que una cláusula de rescisión unilateral sin indemnización no era injusta ni desproporcionada, puesto que la empresa adherente, concesionaria de varias marcas de automóviles, distaba mucho de ser una parte contractualmente débil. ALBIEZ DOHRMANN, Klaus Jochen; *La protección jurídica de los empresarios en la contratación de condiciones generales*, 2009, Navarra, págs. 275 y ss.

237 Así lo establece claramente en su preámbulo la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la contratación, respecto del concepto de cláusula abusiva "tiene así su ámbito propio en la relación con los consumidores. Y puede darse tanto en condiciones generales como en cláusulas predisuestas para un contrato particular al que el consumidor se limita a adherirse. Es decir, siempre que no ha existido negociación individual. 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". Aun lo anterior, también queda claro en el mismo Preámbulo que "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".

238 Art. 1288 del Código Civil: "La interpretación de las cláusulas oscuras de un contrato no deberá favorecer a la parte que hubiere ocasionado la oscuridad".

239 Como ejemplo, el Grupo de expertos en contratos de *Cloud Computing*, de la Comisión Europea. En la Decisión de 18 de junio de 2013 sobre su creación, se estableció que "The Commission intends to facilitate stakeholder agreement promoting the use of safe and fair terms and conditions in cloud computing contracts between cloud computing service providers and consumers and small firms. The Commission should work towards this goal with the active involvement of stakeholders drawing on their expertise and experience in the cloud computing sector" (Considerando 5) y que "The group shall assist the Commission in the identification of safe and fair contract terms and conditions for cloud computing services for consumers and small firms. The group shall take into account existing best

CAPÍTULO SEXTO

Asimismo, algunas normas sectoriales han incluido sistemas de control de contenido en contratos entre empresarios, como la 3/2004 de 29 de diciembre, por la que se establecen Medidas contra la Morosidad en las Operaciones Comerciales, o la Ley 15/2009, de 11 de noviembre, del Contrato de Transporte Terrestre de Mercancías²⁴⁰.

Como bien puntualizan ciertos autores, y como hemos observado en capítulos precedentes²⁴¹, cuando el pequeño empresario prevé destinar los bienes o servicios adquiridos a través de condiciones generales al ejercicio de su actividad profesional, no se puede considerar esta actividad como un acto de consumo en sentido estricto, independientemente de la envergadura de su explotación comercial²⁴². En nuestra opinión, ello no obsta a que el juzgador pueda plantearse la aplicación extensiva de la normativa sobre condiciones abusivas a cláusulas suponga un detrimento injustificado en los derechos o acciones legales de aquellos adherentes pequeños

market practices in contract terms and conditions in cloud computing contracts, as well as the relevant provisions of Directive 95/46/EC" (art. 2). Actualmente, están llevándose a cabo trabajos para desarrollar estas "buenas prácticas" en materia de contratos predispuestos de computación en la nube por consumidores y pequeños empresarios. Asimismo, ALBIEZ DOHRMANN considera unas alternativas más eficaces que otras, en comparación al control de contenidos de las condiciones generales por la legislación específica. ALBIEZ DOHRMANN, Klaus Jochen; *La protección jurídica de los empresarios en la contratación de condiciones generales*, 1ª edición, Navarra, 2009, págs. 293 y ss.

240 Nos referimos a los artículos 9.1 de la Ley de Medidas contra la Morosidad en las Operaciones Comerciales: "1. Será nula una cláusula contractual o una práctica relacionada con la fecha o el plazo de pago, el tipo de interés de demora o la compensación por costes de cobro cuando resulte manifiestamente abusiva en perjuicio del acreedor teniendo en cuenta todas las circunstancias del caso, incluidas: (...)", y los artículos 38.4 "El pacto en contrario se considerará nulo en todos aquellos casos en que tenga un contenido claramente abusivo en perjuicio del porteador y carecerá de efecto cuando se contenga en unas condiciones generales respecto de las que la parte que no las ha propuesto sólo pueda mostrar su aceptación o rechazo global. " y 41.3 "El pacto en contrario se considerará nulo en todos aquellos casos en que tenga un contenido abusivo en perjuicio del porteador, (...)" de la Ley del Contrato Terrestre de Transporte de Mercancías. Al respecto, se ha afirmado que "la promulgación de la LLM [Ley de Medidas contra la Morosidad en las Operaciones Comerciales] en 2004 y de la LCTTM [Ley del Contrato Terrestre de Transporte de Mercancías] en 2009 supuso, a nuestro juicio, la confirmación de que, pese a todo, la inexistencia de mecanismos de control de contenido de las condiciones generales utilizadas en contratos celebrados entre empresarios y profesionales constituía una laguna contraria al plan de la Ley, y que esta laguna podía ser colmada mediante la analogía, extendiendo el control de contenido legalmente formulado respecto de las condiciones generales utilizadas frente a consumidores y usuarios en sentido legal a aquellas que fuesen utilizadas frente a profesionales y empresarios". 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].

241 Ver apartado dedicado al consumidor como destinatario de servicios *cloud*, en el capítulo "Elementos subjetivos del contrato de servicios de computación en la nube".

242 PAGADOR LÓPEZ, Javier, *Condiciones generales y cláusulas contractuales predispuestas*, 1999, Madrid, pág. 193.

CAPÍTULO SEXTO

empresarios que carezcan de conocimientos específicos relacionados con el bien o servicio que adquieren, que además necesiten o dependan en alguna medida de ese bien o servicio, y siempre que se vean impedidos de negociar las cláusulas contractuales. En estos casos, creemos que este pequeño empresario padece una situación de indefensión equiparable a la del consumidor.

De momento, puesto que este déficit legal puede solventarse mediante la analogía entre pequeños empresarios y consumidores, en nuestro país existen algunas sentencias recientes que someten a los controles de transparencia y contenidos ciertas condiciones generales, aunque el contrato con condiciones generales tenga lugar entre profesionales²⁴³.

243 Como ejemplos, el Tribunal Supremo declara en el fundamento cuarto de su sentencia de 18 de junio de 2012 (res. 406/2012) que "el control de inclusión, particularmente referido al criterio de transparencia respecto de los elementos esenciales del contrato, tiene por objeto que el cliente conozca o pueda conocer la carga económica que en conjunto el contrato supone para él y, a su vez, la prestación económica que va a obtener de la otra parte". El voto particular de la sentencia del Tribunal Supremo de 3 de junio de 2016 (res. 367/2016, Magistrado: Fco. Javier Orduña Moreno) destaca la diferencia entre la contratación bajo condiciones generales y la tradicional contratación por negociación, y cuestiona la no extensión del control de transparencia a la contratación bajo condiciones generales entre empresarios, y especialmente, en la que intervienen pequeños y medianos empresarios. Así, afirma el magistrado que "la doctrina jurisprudencial de esta Sala, relativa a la no aplicación del control de transparencia en la contratación entre empresarios o profesionales (fundamento de derecho tercero y cuarto de la sentencia), desatiende el carácter informador del principio jurídico que se deriva del concepto normativo de transparencia, sin que dicha exclusión encuentre tampoco apoyo en la concreción técnica de las variantes que pueden configurar el control de legalidad de la misma (abusividad/incorporación). Por lo que dicha doctrina debe ser rectificada en el sentido de reconocer la aplicación del control de transparencia a la contratación entre empresarios". Por otra parte, la sentencia de la Audiencia Provincial de Córdoba de 18 de junio de 2013 (res. 114/2013), efectuó un control de contenido a una condición general suscrita por un empresario y confirmó la nulidad de una cláusula suelo por abusiva, en un contrato de préstamo con garantía hipotecaria suscrito por una sociedad de responsabilidad limitada, argumentando en su Fundamento noveno que "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". Por otro lado, respecto de la sentencia de la Audiencia Provincial de Alicante, de 11 de julio de 2013 (número de resolución: 394/2013), aunque ninguna de las cláusulas examinadas en el contrato de renting suscrito por una sociedad de responsabilidad limitada fue considerada abusiva por el tribunal, sí fueron sometidas a un control de contenido. La realización por el tribunal de este control de contenido en el marco de un contrato entre profesionales es lo verdaderamente relevante en este caso, y no tanto el resultado de este control. Sin embargo, las recientes sentencias del Tribunal Supremo 246/2014 y 227/2015 no permiten extender el control de contenidos a contratos de adhesión entre empresarios. Aun lo anterior, esta última sentencia reconoce la posibilidad de una aplicación extensiva del control de contenido a contratos suscritos por pequeños empresarios, al afirmar que "el demandado contrató en el sector que en aquel entonces constituía el giro o tráfico habitual de su actividad económica,(...). Por tal razón no procede siquiera entrar a considerar una posible aplicación extensiva o analógica de la protección que el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios otorga a estos al caso de personas físicas comerciantes, empresarios o profesionales cuya actividad económica no pueda considerarse

CAPÍTULO SEXTO

Puesto que la legislación parece negar a los empresarios y profesionales la protección destinada a los consumidores, como norma general se presumen válidas cláusulas generales entre empresarios incluso en aquellas ocasiones en que claramente el profesional adherente se ve perjudicado. Sin embargo, para favorecer su protección, consideramos que puede realizarse una interpretación que integre la regulación contenida en la Ley de Condiciones Generales de la Contratación, (especialmente de la nulidad de cláusulas perjudiciales para el adherente por ser contrarias a la legislación imperativa o prohibitiva de su art. 8.1, y los principios de buena fe y equilibrio contractual, aplicables según su preámbulo respecto de contratos con cualesquiera adherentes, incluso los profesionales²⁴⁴) con los preceptos del Código Civil (concretamente, los artículos 7, 1256 y 1258 que regulan la buena fe contractual; los artículos 1255, 1265 y 1300 que regulan el cumplimiento de la ley, la moral y el orden público; y el artículo 1288 que recoge interpretación en contra de la parte predisponente). Ello sí, teniendo en cuenta siempre las concretas circunstancias de la empresa adherente y su eventual poder de negociación, la capacidad económica del empresario adherente, los conocimientos en la materia y la posibilidad de asesoramiento, la necesidad de adquirir el bien o servicio objeto del contrato, y otras que puedan ser relevantes en cuanto a la creación de un desequilibrio de facto.

En contratos de similares características concluidos con consumidores, los mismos pactos están privados de eficacia al considerarse cláusulas abusivas. Como adelantaron en su momento algunos autores, mediante el concepto restrictivo de

de gran envergadura y que pese a que actúen con un propósito no ajeno a su actividad comercial, empresarial, oficio o profesión, hayan contratado en un sector ajeno al giro o tráfico habitual de su actividad". MIRANDA SERRANO, Luís; PAGADOR LÓPEZ, Javier; *Bienvenidas sean ..., op. cit.*; YÁÑEZ DE ANDRÉS, Aquilino; "Autónomos y pequeños empresarios en la contratación seriada", *Diario La Ley*, núm. 8419, 12 de noviembre de 2014; GUILLÉN CATALÁN, Raquel, "El valor de los votos particulares en la extensión del control de transparencia de la contratación entre empresarios", *Diario La Ley*, núm. 8841, 2016.

244 Preámbulo de la Ley de Condiciones Generales de la Contratación: "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". Compartiendo la opinión de LLODRÁ, hubiera sido aconsejable que se hubiesen incorporado algunas enmiendas propuestas durante los trámites parlamentarios de la Ley de Condiciones Generales de la Contratación, en especial aquellas que extendía a los profesionales la protección contra el uso de cláusulas abusivas. LLODRÁ GRIMALT, Francisca; *El contrato celebrado bajo condiciones generales*, Valencia, 1ª edición, 2002, págs. 346 y ss.

CAPÍTULO SEXTO

consumidor se crea la apariencia de que estos pactos gravosos o perjudiciales son permitidos en contratos entre empresarios, a quienes se les presume el deber de diligencia profesional. Por desgracia, a menudo sucede que la diligencia profesional sucumbe a la necesidad de obtener cierto bien o servicio, con lo cual al adherente pequeño empresario no le queda más opción que acceder a lo establecido por la contraparte o renunciar al preciado bien o servicio²⁴⁵.

En opinión de algunos autores, a la cual nos sumamos, aunque la dinámica del mercado puede incentivar a ofrecer la mejor relación prestación-precio, no sucede lo mismo con las cláusulas contenidas en el contrato, puesto que no suelen tenerse en consideración a la hora de contratar. Conocida esta situación por la parte con mayor fuerza contractual, se utilizan cláusulas predisuestas oscuras por dos razones: la primera, que no existe un riesgo significativo de perder clientes por utilizar condiciones generales desfavorables al adherente (ya que el cliente tiene la necesidad de ese bien o servicio); la segunda, que permiten al proveedor reducir costes, al transmitir riesgos a la otra parte y excluir responsabilidades. Como consecuencia directa de lo anterior, el predisponente podrá ofrecer unos precios más bajos, con lo cual se verá recompensado frente a otros competidores, de forma que, finalmente, el propio mercado acaba incentivando la adopción de cláusulas en perjuicio del adherente²⁴⁶.

Bajo nuestro punto de vista, esta situación tiene lugar de manera reiterada en el mercado de servicios de computación en la nube, donde la mayoría de proveedores coinciden en incluir ciertas cláusulas potencialmente abusivas en los contratos con condiciones generales, los cuales ponen a disposición de un indeterminado número de clientes, sean estos empresarios o consumidores²⁴⁷. De este modo, nos parece que se van consolidando estas prácticas abusivas de forma habitual en el sector, sin que se tenga en cuenta por legisladores y juzgadores la eventual posición de desamparo del adherente profesional y, especialmente, del pequeño empresario. Tengamos en cuenta que el pequeño empresario se encuentra condicionado en el momento de la contratación, debido a la necesidad que le suscita

245 DE CASTRO, F, *Notas sobre las limitaciones intrínsecas a la autonomía de la voluntad. La defensa de la competencia. El orden público. La protección del consumidor*", Anuario de Derecho Civil, 1982, págs. 987 y ss.

246 MIRANDA SERRANO, Luís; PAGADOR LÓPEZ, Javier; *Bienvenidas sean recientes decisiones... op. cit.*

247 Si bien es cierto que muchos proveedores *cloud* diferencian entre servicios dirigidos a empresas y a consumidores, lo cierto es que las cláusulas contractuales utilizadas para la suscripción en línea de estos servicios suelen ser similares.

CAPÍTULO SEXTO

el uso de ciertos servicios tecnológicos que únicamente pueden suscribirse a través de condiciones contractuales no negociadas.

Asimismo, la generalización de contenidos contractuales no negociados y aparentemente gravosos que ofertan distintos proveedores de servicios de computación en la nube que operan en el mercado provoca, a nuestro parecer, una distorsión en la libertad de elección, mediante la cual el desequilibrio entre las partes se mantiene, independientemente del proveedor *cloud* que el adherente profesional elija a la hora de contratar los servicios. Existe un déficit de capacidad negocial que impide equiparar las condiciones generales con las cláusulas examinadas con antelación y negociadas por ambas partes antes de ser aceptadas, que posibiliten la comparación entre proveedores y una elección última que esté sólida y racionalmente fundamentada. Todo ello conduce a que el pequeño empresario no solo ve mermada su posibilidad de elección si esta se basa en el análisis de las condiciones generales predispuestas por los distintos proveedores, sino que, además, si decide contratar con alguno de ellos ese servicio tecnológico (del cual depende en mayor o menor medida) está renunciando a parte de sus derechos y no dispone de cobertura legal que le proteja.

Finalmente consideramos, siguiendo a otros autores²⁴⁸, que sería un buen mecanismo de control de contenido la inclusión legal de una lista de condiciones generales prohibidas para contratos celebrados entre empresarios, equiparable a la enumeración de cláusulas abusivas que recoge el art. 85 del TRDCU, y que se introdujera en la legislación mercantil²⁴⁹. También sería interesante que esta reforma reflejara la realidad del pequeño empresario que contrata en línea, en especial su falta de conocimientos técnicos, la dependencia de aquello que contrata y la imposibilidad de negociar las cláusulas o de acceder a servicios similares en características y precio con unas cláusulas que le sean más beneficiosas.

248 MIQUEL GONZALEZ, José María, "La nulidad de las condiciones generales", en *Las nulidades de los contratos: un sistema en evolución*, (Coord.: J. DELGADO ECHEVERRÍA, Jesús), Navarra, 2007, págs. 193 a 233.

249 En el Anteproyecto de Código Mercantil, aunque recoge un concepto de "condiciones generales" (art. 430-1) y ciertos requisitos de incorporación (incorporación voluntaria de las condiciones por firma o remisión, posibilidad de conocer su contenido, en sus arts. 421-8 y 430-2), se echa en falta un conjunto de normas que permitan efectuar un control de contenido de las condiciones generales, aunque se agradece la previsión de las llamadas cláusulas sorpresivas o imprevisibles (art. 430-3) y la incorporación al texto legal del principio *in dubio, contra proferentem* o en beneficio del adherente (art. 430-4.2). Mientras, en la contratación con consumidores, se aplicará preferentemente la normativa específica.

CAPÍTULO SEXTO

5.- OBLIGACIONES DEL SUSCRIPTOR

Hasta el momento, hemos analizado las obligaciones del proveedor de servicios de computación en la nube. A continuación, observaremos las obligaciones principales de la contraparte, el pequeño empresario que se posiciona jurídicamente como cliente de servicios *cloud*. En el caso de contratos *cloud* onerosos, el pago de una contraprestación dineraria se configurará como la obligación principal del cliente. Veremos cómo, además, de la letra del contrato pueden desprenderse otros deberes accesorios.

5.1.- Pago del precio

En aquellos contratos que se presten a cambio de precio, será esencial determinar de antemano los precios fijos por el uso del servicio, las tarifas con importe variable (por ejemplo, el consumo de recursos) y los precios derivados de eventuales servicios accesorios que se puedan contratar de manera separada.

En los contratos de adhesión, en los cuales hemos centrado este trabajo, el precio no se determinará por negociación, sino al aceptar el cliente la suscripción del servicio porque, entre otras condiciones ofertadas, considera el precio como acorde con el servicio que se le prestará de forma sucesiva.

El proveedor deberá facilitar al cliente pequeño empresario, de acuerdo con el artículo 10.1.f) de la Ley de Servicios de la Sociedad de la Información, "información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío", siendo suficiente con que se incluya en su sitio web y que esté accesible para el cliente de forma permanente, fácil, directa y gratuita (art. 10.2 LSSI)²⁵⁰.

Aunque en su concepción del *Cloud Computing*, el NIST definió como una de sus principales características el pago por consumo de recursos²⁵¹, lo cierto es que, en

250 El proveedor *cloud* está obligado a informar sobre el precio, incluidos impuestos, y los procedimientos de pago a los consumidores, según establece el art. 20 TRLGDCU. En relación a los procedimientos de pago elegidos por el proveedor, cabe decir que no podrá facturarse al cliente cargos que superen el coste que le supone al empresario el uso de tales mecanismos (art. 60 ter TRLGDCU).

251 Este tipo de pago consiste en la de terminación de unidades predefinidas de datos a las que les corresponde un valor [Mb, Tb, etc.], y el precio total resulta de la suma de dichos valores. SOLER MATUTES, Pere, *El contrato para la elaboración de programas de ordenador. El programa de desarrollo de software*. 2003, Navarra, pág. 200. Este tipo de precio permite reflejar la característica escalabilidad de los servicios de computación en la nube. Frecuente en servicios de

CAPÍTULO SEXTO

la práctica, la determinación del precio tiene lugar, además, a través de otros mecanismos. Por ejemplo, el pago por ciertas funcionalidades, a modo de tarifas planas (que pueden llevar asociado el consumo libre de recursos hasta un límite determinado)²⁵², o el pago por número de usuarios con derecho a utilizar el servicio²⁵³. Todos estos sistemas, así como cualesquiera otros que pueda proponer el prestador de servicios²⁵⁴, son, en principio, válidos de acuerdo con la libre fijación de precios al amparo del principio de la libre autonomía y del artículo 17 de la Ley 3/1991, de 10 de enero, de Competencia Desleal²⁵⁵. Al tratarse de un contrato de tracto sucesivo, el pago se realiza con periodicidad (mensual, trimestral, anual, etc.).

Por otra parte, puede pactarse, dependiendo del servicio, el pago por ciertas funcionalidades accesorias²⁵⁶, como los servicios de integración o el acceso a herramientas o prestaciones complementarias²⁵⁷. Si bien para la contratación de estos servicios opcionales se necesitará el consentimiento expreso del cliente consumidor (art. 60 TRLGCDU), la LSSI no añade ningún otro requisito sobre información al pequeño empresario más allá del mencionado artículo 10.1. f), como tampoco lo hace el Código Civil²⁵⁸.

La contraprestación dineraria determinada inicialmente por el servicio *cloud* puede presentar reducciones o exenciones de pago cuando entren en juego los mencionados créditos de servicio, en algunos de los cargos periódicos efectuados al cliente. Operarán en aquellos casos determinados en el contrato, generalmente al incumplirse alguno de los objetivos del acuerdo de nivel de servicio²⁵⁹.

infraestructura como servicio (IaaS) de suministro de capacidades informáticas (*megabytes* transferidos, máquinas virtuales utilizadas, capacidad de procesamiento consumida, etc.).

252 Muy habitual en softwares como servicio (SaaS) de correo electrónico, en los cuales el cliente dispone de una determinada capacidad de almacenamiento remoto de mensajes.

253 Por ejemplo, en de SaaS (Software como Servicio) *Customer Relationship Management* o CRM para empresas, del tipo *Salesforce*.

254 Por ejemplo, determinación de precios según franja horaria.

255 Art. 17 Ley 3/1991, de 10 de enero, de Competencia Desleal: "Salvo disposición contraria de las leyes o de los reglamentos, la fijación de precios es libre. (...)".

256 Por ejemplo, pagos por uso de ciertas herramientas de análisis de datos.

257 Habitual en herramientas *PaaS (Plataforma como Servicio)* de desarrollo de aplicaciones informáticas.

258 Art. 60 TRLGDCU: "Antes de que el consumidor y usuario quede vinculado por cualquier contrato u oferta, el empresario deberá obtener su consentimiento expreso para todo pago adicional a la remuneración acordada para la obligación contractual principal del empresario. Estos suplementos opcionales se comunicarán de una manera clara y comprensible y su aceptación por el consumidor y usuario se realizará sobre una base de opción de inclusión. Si el empresario no ha obtenido el consentimiento expreso del consumidor y usuario, pero lo ha deducido utilizando opciones por defecto que éste debe rechazar para evitar el pago adicional, el consumidor y usuario tendrá derecho al reembolso de dicho pago".

259 Ver apartados "El cumplimiento defectuoso y la determinación de *service credits* como

CAPÍTULO SEXTO

Asimismo, es posible que la contraprestación del cliente sea no dineraria, aunque ello no implique que carezca de valor económico, como sucede con aquellos contratos ofrecidos como "gratuitos" pero que se prestan a cambio de cesiones de datos personales o de derechos de propiedad intelectual. Sin embargo, como se ha afirmado, esta falta de contraprestación dineraria no supone que el contrato carezca de consecuencias jurídicas para las partes²⁶⁰.

5.2.- Otras obligaciones del cliente

El contrato de servicios de computación en la nube puede suponer la asunción de otros deberes y cargas accesorios que sirven de contraprestación junto al pago del precio por parte del cliente. Entre ellos, destacamos en los siguientes apartados los deberes de colaboración con el proveedor y el cumplimiento con la política de uso adecuado del servicio impuesta por el proveedor.

5.2.1- La existencia de un deber de colaboración con el proveedor

Dentro de las Políticas de Uso Adecuado²⁶¹, bajo las cuales el cliente se compromete a usar el servicio, a menudo se exige un deber de colaboración que, por otra parte, resulta implícito al propio contrato de servicios²⁶². De este modo, las consecuencias establecidas contractualmente para el incumplimiento de la política de uso también se devengarán en aquellos casos en los cuales el cliente entorpezca el servicio (arts. 1101, 1102, 1103 y 1106 del Código Civil), teniendo en cuenta, para determinar el daño, la incidencia que haya tenido el incumplimiento en la puesta en compromiso de la accesibilidad, rendimiento o seguridad del sistema, y si esa utilización indebida ha causado daños y perjuicios al proveedor o a terceros usuarios (art. 1902 del Código Civil).

Como hemos observado en anteriores capítulos, el proveedor aparece como única autoridad decisoria sobre la determinación de consecuencias de tal incumplimiento, que generalmente son la suspensión o terminación del servicio (con

indemnización al cliente", en este mismo capítulo.

260 Ver apartado sobre onerosidad, en el capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube". 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.

261 Ver apartado "Las PUA en los contratos de computación en la nube", en el capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

262 APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática...*, *op. cit.*, pág. 123.

CAPÍTULO SEXTO

o sin aviso previo) y la eventual responsabilidad por daños ocasionados al obstaculizar o impedir la adecuada prestación del servicio²⁶³. Asimismo, el proveedor puede exigir al cliente el cumplimiento de lo acordado o la resolución del contrato (art. 1124 del Código Civil).

Cuando la adecuación del servicio a las necesidades del cliente dependa de la recomendaciones que pueda hacerle el proveedor (por ejemplo, en relación con su operativa negocial, la sensibilidad de los datos que maneja, problemas técnicos que padece, etc.), será conveniente que el cliente pequeño empresario tenga conocimiento de las informaciones que precisa aportar al proveedor, aunque siempre es deseable que este deber tenga reflejo contractual²⁶⁴. Así, el cliente destinatario del servicio tiene el deber de informar al proveedor *cloud* de peculiaridades que puedan afectar a la prestación, por ejemplo, el manejo de datos especialmente sensibles o de cargas de trabajo muy exigentes. Este deber está estrechamente vinculado con su deber de colaboración y con el principio de buena fe contractual²⁶⁵. Así, como afirman algunos autores y como se deriva del principio de responsabilidad negocial, el ordenamiento exige al cliente informarse de las circunstancias de hecho que le interesan en relación al futuro contrato, y si es necesario, deberá solicitar del proveedor información complementaria. Si el cliente *cloud* pequeño empresario omite estas precauciones, podría contradecir el principio de buena fe contractual o puede faltar al deber de diligencia que, como profesional, le es exigible²⁶⁶.

5.2.2.- Legalidad y pertinencia de los contenidos, cumplimiento de las PUA, y buena fe contractual

En capítulos anteriores hemos definido la política de uso adecuado (o PUA) como "aquel conjunto de cláusulas que regulan la manera en la que los clientes deben usar el servicio, así como determinadas acciones prohibidas"²⁶⁷. Por tanto, puesto que forma parte del contenido contractual al cual se ha comprometido el cliente, le será exigible en toda su extensión. Si el proveedor detecta un comportamiento del cliente que contravenga las disposiciones de la política de uso adecuado, podrá adoptar las consecuencias que

263 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".

264 APARICIO VAQUERO, Juan Pablo, *La nueva contratación...*, *op. cit.*, pág. 125.

265 Ver "Obligaciones del cliente", en este mismo capítulo".

266 CORRIPIO GIL-DELGADO, M^a Reyes, *El deber de información precontractual*, Madrid, 1999, pág. 273.

267 Definición propia. Ver apartado "Las PUA en los contratos de computación en la nube", en el capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

CAPÍTULO SEXTO

contractualmente se prevean ante tal incumplimiento. Estas consecuencias dependerán en gran medida de cada proveedor, al ser quien predispone las condiciones generales para su suscripción, y pueden abarcar desde la suspensión o terminación del servicio para el presunto infractor mientras se investigan los hechos, hasta la asunción de responsabilidades por daños causados al proveedor o a terceros y derivados de la realización de actividades no permitidas.

La comunicación de presuntos usos ilegítimos o de existencia de contenidos ilegales realizada por otros usuarios es un buen mecanismo para controlar el cumplimiento general de las políticas de uso adecuado a disposición de los proveedores. Dependiendo del contrato, esta colaboración del usuario puede configurarse como una obligación con el proveedor, aunque consideramos más bien que es una facultad en interés del buen uso del servicio por la comunidad de beneficiarios, puesto que su inobservancia por el suscriptor no suele derivar en consecuencias.

CAPÍTULO SÉPTIMO

Capítulo Séptimo

MODIFICACIÓN, SUSPENSIÓN Y EXTINCIÓN DEL CONTRATO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

1.- INTRODUCCIÓN

La modificación de la prestación y la extinción de los contratos de computación en la nube, cuestiones que abordamos en este capítulo, presentan ciertas particularidades. Por una parte, en la práctica del sector podemos encontrarnos con reservas que efectúa el proveedor en relación a la continuidad del servicio o a la modificación de la prestación, en ocasiones sin necesidad de justificación o preaviso, o sin que tenga lugar un procedimiento transparente que permita al cliente efectuar alegaciones al respecto. Recordemos que, como se ha visto, estas condiciones no son negociables en la mayoría de ocasiones por el cliente que tenga la condición de pequeño empresario.

Por otra parte, una vez extinguida la relación contractual, es imprescindible para la empresa suscriptora del servicio conocer el destino de sus datos, poder recuperarlos o trasladarlos a sistemas de otro proveedor sin tener que volver a introducirlos manualmente en el sistema informático, así como contar con garantías de que el proveedor eliminará esos datos definitivamente una vez transcurrido el plazo legal que le exija conservarlos en sus sistemas. En las siguientes páginas, por tanto, centraremos nuestra atención en los supuestos de suspensión, modificación

CAPÍTULO SÉPTIMO

unilateral y extinción del servicio, y en las consecuencias de la finalización del nexo contractual entre ambas partes.

Dos razones derivadas de la naturaleza del servicio motivan la existencia de cláusulas que permiten modificar tanto la prestación del servicio como el contenido contractual. La primera razón es el hecho de que el servicio consista en el suministro de capacidades computacionales, sustentado en la tecnología informática. La segunda razón es la concepción del *Cloud Computing* como un servicio cuya prestación se configura de manera continuada e ininterrumpida en el tiempo, reflejándose en contratos suscritos por plazo indefinido o que permiten prórrogas automáticas. Todo ello implica una evolución y actualización constante del estado de la técnica, y este dinamismo podrá reflejarse en las características del servicio que el proveedor esté interesado en ofertar comercialmente, así como en las necesidades del cliente pequeño empresario, las cuales pueden variar en el transcurso de la relación contractual.

El proveedor, además, puede reservarse el derecho a suspender la prestación. Aunque existen causas que podrían legitimar al proveedor a suspender el servicio al cliente, como por ejemplo el incumplimiento de la obligación de pago por este último, tras comunicarse al cliente su situación de morosidad, a menudo las cláusulas amparan también otros incumplimientos contractuales, como sucede cuando el cliente realiza actividades contrarias a las políticas de uso adecuado del servicio (o PUA). Pero, en ocasiones, las cláusulas van más allá y permiten al proveedor la suspensión o cancelación del servicio sin necesidad de alegar justa causa.

Al igual que en los supuestos de modificación unilateral de las condiciones, será relevante la causa de la suspensión y el modo en el cual se le comunica al cliente, así como el margen otorgado de reacción antes de que tenga lugar la cancelación definitiva del servicio. En todos estos casos, el proveedor aparece como único enjuiciador que examina y decide sobre tal continuidad, con lo cual el cliente puede ver mermada su facultad de alegación y defensa, y su actividad empresarial puede obstaculizarse gravemente debido a una súbita detención del suministro de la capacidad contratada¹. En este capítulo, observaremos las diferentes causas que

1 Imaginemos la dificultad que supone para una empresa quedarse sin servicios como correo electrónico, o que se deniegue su acceso a programas informáticos de manejo de datos de clientes o empleados, o a datos empresariales que se almacenan remotamente y se comparten entre personal o clientela. Como vemos, con la prestación del servicio se crea una dependencia del servicio, y no

CAPÍTULO SÉPTIMO

motivan una modificación del contenido contractual y/o de la continuidad de la prestación, y reflexionaremos sobre su admisibilidad y validez legal.

También en posteriores apartados analizaremos las principales causas que puedan llevar a la extinción definitiva de la relación jurídica entre las partes del contrato de computación en la nube: el desistimiento, la resolución por incumplimiento y la imposibilidad por fuerza mayor o caso fortuito. Si bien son importantes estas causas y la manera en que vienen recogidas en la letra del contrato (especialmente por su relación con la distribución de riesgos y las limitaciones y exoneraciones de responsabilidades en ciertos casos), la verdadera relevancia práctica radica en los efectos que la terminación del contrato tiene sobre la información migrada.

Así, la portabilidad de los datos y de las aplicaciones implica aspectos cuyo conocimiento puede resultar relevante para el cliente pequeño empresario, como la descripción del proceso de portabilidad, el formato de recuperación de los datos y el tiempo del cual dispondrá el cliente para su rescate, si el proveedor facilitará asistencia durante el proceso de transición hacia otro proveedor, o si supondrá costes adicionales. Una vez transferidos los datos migrados durante el transcurso de la prestación, el proveedor puede retenerlos durante un período (por ejemplo, por motivos legales) o puede proceder a su borrado inmediato. Asimismo, la puesta en conocimiento del cliente del periodo de retención de datos y los mecanismos de borrado son relevantes jurídicamente, no solo a efectos de los deberes de información y diligencia entre las partes, sino también en materia de cumplimiento de la normativa sobre protección de datos de carácter personal.

A continuación, procederemos al estudio de las cuestiones que hemos avanzado.

2.- LA MODIFICACIÓN DE CLÁUSULAS CONTRACTUALES

La permanente necesidad evolutiva de la técnica informática supone que, para permitir la competitividad, avances y eficacia de la computación en la nube, deban adoptarse cambios en la estructura, funcionalidades y desempeño de los servicios que

siempre resulta fácil un cambio de proveedor.

CAPÍTULO SÉPTIMO

proporcionan los diferentes proveedores. Estos cambios suelen motivar un tipo de cláusulas, muy habituales en los contratos de computación en la nube, en las cuales el proveedor se reserva el derecho a modificar diferentes aspectos del servicio². El uso de estas cláusulas no es exclusivo de contratos de servicios *cloud*, sino que también son comunes en diferentes contratos de servicios en línea³. Los cambios efectuados unilateralmente por el proveedor pueden ser de distinta naturaleza, y responder a modificaciones de los cometidos de los recursos suministrados; a aspectos relacionados con el rendimiento del servicio; o pueden alterar las condiciones contractuales inicialmente suscritas por el cliente⁴.

En los contratos de computación en la nube, el grupo de expertos de la *Cloud Computing Strategy* resalta dos problemas concretos derivados de las condiciones generales que permiten modificar unilateralmente el contrato⁵. En primer lugar, la

2 BRADSHAW, S; MILLARD, C; WALDEN, I, "Standard contracts for Cloud Services", *Cloud Computing Law*, (Coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 54.

3 DLA Piper UK LLP, *Comparative Study on Cloud Computing Contracts. Final Report for European Commission* [en línea], 2015, pág. 54. Disponible en: <http://ec.europa.eu/justice/contract/cloud-computing/studies-data/index_en.htm>. [Fecha de consulta: 9 de febrero de 2017].

4 Esta cláusula parece ser verdaderamente operativa, y que los proveedores modifican a menudo tanto aspectos relacionados con el servicio como con las cláusulas contractuales. Así, según asegura el sitio web *terminosycondiciones.es* creado por el jurista Jordi Morell, que monitoriza las modificaciones de todo tipo efectuadas en condiciones generales de servicios informáticos suscritos en línea, entre ellos cláusulas de adhesión propuestas por diferentes proveedores *cloud*, durante el año 2016 se detectaron 10.512 cambios en las aproximadamente 7.100 políticas de condiciones y privacidad monitorizadas por sus herramientas de rastreo. Entre los proveedores que más cambios realizaron en sus condiciones en 2016, destaca el proveedor de servicios de *cloud* y *hosting* Arsys (con 107 cambios de todo tipo), y las redes sociales *Twitter* y *Facebook* (con 88 y 79 cambios respectivamente). Respecto de los cambios relevantes efectuados sobre el total de textos legales según el sitio web, un 55% de cambios relevantes se comunicaron a los usuarios, mientras que el 45% restante se realiza sin notificarlo al usuario e, incluso, sin modificar la fecha de la última actualización del texto legal. Septiembre de 2016 fue el mes con más repunte de modificaciones, 1558, como resultado de la entrada en vigor del Escudo de Privacidad o *Privacy Shield* (ver capítulo "Privacidad en la nube: principales cuestiones de carácter personal" al respecto de las transferencias internacionales, en este mismo trabajo). Para más información, nos remitimos a los datos de 2016 publicados por la web, puesto que los datos referentes al año 2017 no han sido publicados en el momento de elaboración de este trabajo. Disponible en: <<https://terminosycondiciones.es/2017/01/11/asi-cambiaron-diez-mil-veces-los-terminos-condiciones-2016/>>. [Fecha de consulta: 9 de febrero de 2017].

5 En este informe, redactado por YANGUAS GÓMEZ dentro del marco de la *Cloud Computing Strategy* de la Comisión Europea, se pone de manifiesto la habitualidad y la problemática del uso de las cláusulas de modificación unilateral en contratos de computación en la nube. *Discussion Paper on Modifications on Cloud Computing Contracts* [en línea]. Disponible en:

CAPÍTULO SÉPTIMO

falta de transparencia en relación a los motivos que fundamentan las eventuales modificaciones, y, en segundo lugar, las formas en las cuales el proveedor comunica tales cambios (actualización de los términos en la página web del proveedor, envío de correos electrónicos, o a través de otros métodos⁶), o si no comunica los cambios al cliente, y las razones que le permiten considerar que el cliente ha aceptado los nuevos parámetros.

En todos los casos, será relevante la letra de cada una de las cláusulas referentes a la modificación del contenido contractual, para determinar si son o no equitativas, puesto que existen notables diferencias entre las redacciones de uno y otro proveedor.

2.1.-Las modificaciones del servicio y las modificaciones de las condiciones contractuales

En cuanto a los cambios en aspectos funcionales del servicio, si se aumentan las funcionalidades inicialmente suscritas, o si se mejora su rendimiento, no suelen darse mayores problemas. Sin embargo, la situación cambia cuando el proveedor decide reducir notablemente su eficiencia. Recordemos que las condiciones generales suscritas suelen reservar al proveedor esta facultad, pudiendo introducir tales cambios sin preaviso ni motivación, libre y unilateralmente, lo cual, en última instancia, puede suponer una modificación del objeto, núcleo de la relación contractual, sin mediar un efectivo consentimiento mutuo.

Al respecto, veamos una muestra de estas condiciones generales:

"[El proveedor] podrá realizar publicaciones en el sitio y/o enviar un mensaje de correo electrónico a la dirección principal asociada a su cuenta para enviar notificaciones de cualquier cambio material en los servicios. Su responsabilidad es revisar su dirección de correo electrónico y/o la dirección de correo electrónico principal que ha registrado en [el proveedor] para recibir dichas notificaciones. Reconoce que [el proveedor] no es responsable ante usted ni ante ningún tercero de cualquier modificación, cese o interrupción de los servicios. Si ha pagado por utilizar los servicios y los damos por finalizados sin ningún motivo o reducimos considerablemente

<http://ec.europa.eu/justice/contract/files/expert_groups/modification_contracts_en.pdf>. [Fecha de consulta: 9 de febrero de 2017]

6 Por ejemplo, la red social *Twitter* afirma enviar *twits* a sus usuarios, con los contenidos de las reformas, mientras que la red social *Facebook* permite a sus usuarios seguir las actualizaciones de las condiciones activando la pestaña *Me gusta* de la *Facebook Site Governance Web Page*.

CAPÍTULO SÉPTIMO

su funcionalidad, le reembolsaremos el importe prorrateado de cualquier pago anticipado, según lo consideremos apropiado"⁷.

A nuestro parecer, y teniendo en consideración el ordenamiento jurídico español, esta cláusula implica un desequilibrio injustificado entre las partes. Como podemos observar, en esta cláusula, el proveedor se reserva el derecho a alterar las funcionalidades del servicio, o de interrumpir el propio servicio, de manera totalmente libre y sin necesidad de motivación⁸. Además, será el proveedor quien decida si notifica *a priori* o *a posteriori* esos cambios al cliente, o si no los notifica. Igualmente, será el proveedor quien decida si devolverle o no el importe ya abonado por pagos anticipados. Por contrapartida, esta cláusula supone para el cliente las cargas de revisar y mantener actualizada su dirección de correo electrónico, e incluso, si así lo decide el proveedor, de soportar esa reducción de funcionalidad sin reembolso de pagos ya efectuados. Nos encontraríamos, en este último caso, ante un enriquecimiento injusto del proveedor, y, por contrapartida, ante una situación de indefensión del cliente pequeño empresario, o ante una cláusula abusiva si quien ha suscrito el contrato de computación en la nube es un consumidor⁹.

Bajo nuestro punto de vista, si bien podría ser aceptable que no se informe al cliente de modificaciones que afecten mínimamente al rendimiento o a otras características técnicas, opinamos que, si se produce un cambio relevante en aspectos técnicos del servicio, independientemente de que afecte o no de manera adversa al cliente, debería, en primer lugar, efectuarse una notificación previa al cliente que le permitiera conocer la existencia de esa futura modificación, y, en su caso, de ponderar la necesidad o el coste de adaptarse a esos cambios y continuar con el

7 Condiciones de uso del software como servicio *Box* [en línea]. Disponible en: <<https://www.box.com/legal/termsofservice/ES/>>. [Fecha de consulta: 9 de febrero de 2017].

8 Las interrupciones y suspensiones del servicio se tratarán en apartados posteriores de este mismo capítulo.

9 Concretamente, serían potencialmente abusivas las cláusulas que permitan modificaciones unilaterales que "reserven a favor del empresario facultades de interpretación o modificación unilateral del contrato, salvo, en este último caso, que concurran motivos válidos especificados en el contrato" (art. 85.3 TRLGCU), que "supongan la concesión al empresario del derecho a determinar si el bien o servicio se ajusta a lo estipulado en el contrato" (art. 85.11 TRLGDCU), que supongan "la exclusión o limitación de forma inadecuada de los derechos legales del consumidor y usuario por incumplimiento total o parcial o cumplimiento defectuoso del empresario (...)" (art. 86.1), o "la limitación o exclusión de la facultad del consumidor y usuario de resolver el contrato por incumplimiento del empresario" (art. 86.5 TRLGDCU), y "la imposición de obligaciones al consumidor y usuario para el cumplimiento de todos sus deberes y contraprestaciones, aun cuando el empresario no hubiere cumplido los suyos" (art. 87.1).

CAPÍTULO SÉPTIMO

servicio, o si le conviene comparar ofertas de distintos proveedores.

En segundo lugar, el proveedor debería ofrecer al cliente la oportunidad de rescindir el contrato, especialmente cuando exista una diferencia entre lo inicialmente contratado y lo posteriormente recibido que suponga para el cliente una significativa reducción de beneficios o prestaciones. En este caso, opinamos que debería considerarse, respecto del objeto del contrato, si bajo esta modificación del servicio subyace un incumplimiento parcial de la prestación por parte del proveedor. Atendiendo a la interpretación conjunta del contrato, deberá contemplarse, en primer lugar, la validez de esta cláusula de modificación unilateral del objeto contractual, valorando si procede su nulidad por ser una disposición desequilibrada y contraria al deber de diligencia profesional y al principio de buena fe contractual¹⁰. Además, consideramos que el contrato debería indicar si existe la posibilidad de una rescisión sin penalización por no conformidad con la reducción o modificación en las prestaciones e, incluso, si se puede recibir algún tipo de compensación o reducción del precio acorde con la disminución de funcionalidades.

Igualmente, cuando el proveedor se reserva el derecho de efectuar cambios en aspectos relacionados con el servicio contratado, a menudo tal reserva no abarca solo aspectos materiales del servicio, sino también la modificación unilateral de condiciones contractuales. A continuación, abordaremos este segundo aspecto¹¹.

10 Consideramos que debe realizarse una interpretación global del contenido contractual, poniendo especial atención en si el adherente es consumidor o empresario, si se trata de un contrato sujeto o no a contraprestación económica, y en las limitaciones o exenciones de responsabilidad efectuadas por el proveedor.

11 Seguidamente, podemos observar una cláusula de reserva de modificación unilateral de condiciones contractuales: "Es posible que cambiemos estas condiciones de vez en cuando debido a los cambios que se realizan en nuestros servicios y las leyes que se aplican a usted y a nosotros. Fecharemos y publicaremos la versión más reciente de estas condiciones en el sitio. Si realizamos algún cambio, se lo notificaremos modificando la fecha de «Última modificación» en la parte superior de estas condiciones y, según sea apropiado, podríamos enviarle un aviso adicional (por ejemplo, añadiendo un comunicado en la página inicial o enviándole una notificación por correo electrónico). Los cambios efectuados empezarán a surtir efecto en el momento de la publicación en los servicios de la versión modificada de estas condiciones (o en otra fecha de entrada en vigor posterior indicada en el encabezamiento de las condiciones modificadas). Si a nuestro juicio las modificaciones de estas condiciones son importantes, se las notificaremos por medio de los Servicios o enviándole un mensaje a la dirección de correo electrónico asociada a su cuenta. La notificación de otros cambios podrá realizarse en el Sitio o los blogs de BOX relacionados. Por lo tanto, le instamos a que compruebe la fecha de estas condiciones cada vez que visite el Sitio para saber si se han actualizado. Si actualizamos estas condiciones y usted no está de acuerdo con los cambios, deberá decidir libremente si las acepta o deja de utilizar los servicios. Puede desactivar su cuenta en cualquier momento en los ajustes de «Su cuenta». Si continúa accediendo a los servicios o usando cualquier parte de los mismos, se entiende que acepta los cambios de las condiciones. Si no acepta alguno de esos cambios, no estamos obligados a seguir

CAPÍTULO SÉPTIMO

Como es sabido, en nuestro ordenamiento los acuerdos contractuales tienen fuerza de ley entre las partes (art. 1091 del Código Civil¹²), y pueden modificarse y sustituirse por nuevos pactos (arts. 1203 y 1204 del Código Civil¹³) bajo la regla general del mutuo acuerdo, con lo cual no debe dejarse al arbitrio de una de las partes contractuales la validez y ejecución del contrato¹⁴ (art. 1256 del Código Civil).

Tanto en las relaciones interempresariales como en los contratos con consumidores, las partes pueden acordar la modificación unilateral de cláusulas (art. 1255 del Código Civil¹⁵). Sin embargo, estas cláusulas son susceptibles de ser consideradas abusivas según la normativa de protección al consumidor (arts. 85.3 y 85.5 TRLGDCU¹⁶), cuando no concurren motivos válidos especificados en el contrato¹⁷. Los pequeños empresarios, en principio, deberán asumir lo acordado en el pacto¹⁸.

Los motivos que fundamenten tales cambios pueden consistir en adaptaciones a nuevas legislaciones, a motivos comerciales o a exigencias de la evolución técnica

proporcionándole los servicios, y debe cancelar los servicios y dejar de usarlos". Condiciones de uso del software como servicio de almacenamiento remoto de datos Box [en línea]. Disponible en: <<https://www.box.com/legal/termsofservice/ES/>>. [Fecha de consulta: 9 de febrero de 2017].

- 12 Art. 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".
- 13 Código Civil. Art. 1203: "Las obligaciones pueden modificarse: 1.º Variando su objeto o sus condiciones principales. 2.º Sustituyendo la persona del deudor. 3.º Subrogando a un tercero en los derechos del acreedor". Art. 1204: "Para que una obligación quede extinguida por otra que la sustituya, es preciso que así se declare terminantemente, o que la antigua y la nueva sean de todo punto incompatibles".
- 14 Art. 1256 del Código Civil: "La validez y el cumplimiento de los contratos no pueden dejarse al arbitrio de uno de los contratantes".
- 15 Art. 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".
- 16 Art. 85 del Texto Refundido que aprueba la Ley General para la Defensa de Consumidores y Usuarios y otras leyes complementarias. "Las cláusulas que vinculen cualquier aspecto del contrato a la voluntad del empresario serán abusivas y, en todo caso, las siguientes: (...) 3.- Las cláusulas que reserven a favor del empresario facultades de interpretación o modificación unilateral del contrato, salvo, en este último caso, que concurren motivos válidos especificados en el contrato.(...) .5.- "Las cláusulas que determinen la vinculación incondicionada del consumidor y usuario al contrato aún cuando el empresario no hubiera cumplido con sus obligaciones".
- 17 Para determinar la posible abusividad de la cláusula deberemos poner atención, pues, en lo que puede entenderse como "motivos válidos especificados en el contrato", es decir, a la introducción en el contrato de la posibilidad de modificación de las cláusulas y de que esos cambios se entiendan válidos por entenderse razonables y que no perjudican al consumidor.
- 18 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 este mismo trabajo.

CAPÍTULO SÉPTIMO

del sector, con lo cual no serán válidas aquellas modificaciones meramente arbitrarias o no razonables¹⁹. Respecto de los motivos comerciales, consideramos que deberá garantizarse el equilibrio de las prestaciones entre cliente y proveedor, y deberá darse la oportunidad al suscriptor de rescindir el contrato en el caso que de no esté conforme con los cambios realizados.

Aunque es razonable esperar que puedan adoptarse cambios en servicios *cloud* suscritos con duración indefinida o que se renuevan automáticamente, cabe la posibilidad de que la redacción de estas cláusulas permita amparar modificaciones de muy diverso calibre que el proveedor estime conveniente adoptar, como mejoras técnicas o un ajuste de los precios²⁰. Algunas modificaciones se consideran legítimas en los contratos de tracto sucesivo y larga duración, por ejemplo aquellas que permiten mejoras técnicas, o un ajuste de los precios²¹.

19 A continuación, un ejemplo de motivos recogidos en las propias condiciones generales. Se trata del contrato del software como servicio (SaaS) de almacenamiento remoto *OneDrive* de Microsoft: "Actualizaciones de los Servicios o el Software y Cambios en Estos Términos. a. Cuando vayamos a cambiar estos Términos, le informaremos. Podemos modificar estos Términos debido a (i) la legislación aplicable, incluida, sin limitarse a ello, una modificación de la ley; (ii) una recomendación o requerimiento conforme a la legislación aplicable; (iii) la evolución de los Servicios; (iv) motivos técnicos; (v) requisitos operativos o (vi) una modificación de los términos en beneficio del usuario". Condiciones del servicio *Onedrive* [en línea]. Disponibles en: <<https://www.microsoft.com/es-es/servicesagreement/>>. [Fecha de consulta: 22 de mayo de 2017].

20 Básicamente, con estas cláusulas el proveedor *cloud* se reserva la posibilidad de modificar cualquier cláusula contractual (tarifas, funciones del servicio, cesiones de contratos, etc.). En el artículo 47 b) de la Ley General de Telecomunicaciones, en el cual se atribuye al operador la facultad para modificar las condiciones de prestación del servicio sin necesidad de requerir el consentimiento del usuario contratante, aunque se le exige que tal modificación se sustente en "motivos válidos" y que el cliente tenga la facultad de resolver el contrato sin penalización en caso de disconformidad: "El derecho [del usuario final de redes y servicios de comunicaciones electrónicas] a resolver el contrato en cualquier momento. Este derecho incluye el de resolverlo anticipadamente y sin penalización en el supuesto de modificación de las condiciones contractuales impuestas por el operador por motivos válidos especificados en aquél y sin perjuicio de otras causas de resolución unilateral". Sería ideal que lo mismo pudiera exigírseles a los proveedores de computación en la nube. Respecto de modificaciones de contratos con consumidores en servicios de telecomunicaciones, nos remitimos a MENDOZA LOSANA, Ana I, *Ofertas "para toda la vida" y modificación de condiciones de los contratos de servicios de telecomunicaciones*, Consulta al Centro de Estudios de Consumo de la Universidad de Castilla La Mancha, [en línea]. Disponible en: <<https://www.uclm.es/centro/cesco/pdf/trabajos/29/ofertastodavida.pdf>>. [Fecha de consulta: 13 de febrero de 2017].

21 El Tribunal de Justicia de la Unión Europea, en su sentencia de la Sala Primera, de 21 de marzo de 2013, asunto C-92/11, en relación a los contratos de adhesión entre un profesional y un consumidor, declara que: "para apreciar si una cláusula contractual tipo, mediante la que una empresa suministradora se reserva el derecho a modificar el coste del suministro de gas, obedece o no a las exigencias

CAPÍTULO SÉPTIMO

En el ámbito de la legislación de protección al consumidor, la normativa comunitaria prevé como abusivas las cláusulas que permitan modificar unilateralmente las previsiones contractuales y las condiciones del servicio que provoquen un desequilibrio considerable en detrimento del consumidor y que no sustenten en motivos válidos. Así se recoge en el anexo de la Directiva 93/13/CE, letras j) y k) de la Directiva del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores. Esta afirmación aparece matizada en la misma Directiva, en relación a la existencia de cláusulas de modificación unilateral en contratos de duración indefinida, al reconocerse que estas cláusulas son aceptables, siempre y cuando el proveedor informe al consumidor de manera previa, y que le ofrezca la opción rescindir el contrato dentro de un plazo de tiempo razonable (párrafo 2b) del mismo Anexo)²². Consideramos que sería deseable

de buena fe, equilibrio y transparencia que imponen tales disposiciones, reviste concretamente una importancia esencial determinar: [1.-] Si en el contrato se expone de manera transparente el motivo y el modo de variación de tal coste, de forma que el consumidor pueda prever, sobre la base de criterios claros y comprensibles, las eventuales modificaciones de ese coste. La falta de información a este respecto antes de celebrarse el contrato no puede ser compensada, en principio, por el mero hecho de que el consumidor será informado, durante la ejecución del contrato, de la modificación del coste con una antelación razonable y de su derecho a rescindir el contrato si no desea aceptar la modificación, y [2.-] Si la facultad de rescisión conferida al consumidor puede, en la situación concreta, ser ejercida efectivamente". En otras palabras, se reconoce el interés de las empresas a modificar unilateralmente los precios, pero declara abusiva la cláusula contractual suscrita por consumidores que prive a estos últimos último de conocer y prever el motivo de las causas y variación del precio, y de la facultad de rescindir el contrato y cambiar de proveedor. Para un estudio más detallado sobre modificaciones unilaterales de los precios en contratos bajo condiciones generales, nos remitimos a MENDOZA LOSANA, Ana I, "Control de condiciones generales de la contratación en sectores regulados. En particular, la cláusula que permite la modificación unilateral de los precios", *Centro de Estudios de Consumo de la Universidad de Castilla la Mancha* [en línea]. Disponible en: <<https://www.uclm.es/centro/cesco/pdf/trabajos/30/22.pdf>>. [Fecha de consulta: 13 de febrero de 2017].

- 22 El art. 3.1 de la mencionada Directiva afirma que "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". En su Anexo, la Directiva contiene un listado de cláusulas que pueden ser consideradas abusivas. Al respecto de la reserva del proveedor del derecho a introducir modificaciones unilaterales en el servicio o en las condiciones contractuales, cabe destacar las siguientes: "j) autorizar al profesional a modificar unilateralmente sin motivos válidos especificados en el contrato los términos del mismo; k) autorizar al profesional a modificar unilateralmente sin motivos válidos cualesquiera características del producto que ha de suministrar o del servicio por prestar;(…)". La exigencia de que esta cláusula se comunique previamente y con antelación en contratos indefinidos con consumidores aparece en el apartado 2b) del Anexo, en estos términos: "La letra j) se entiende sin perjuicio también de las cláusulas por las que el profesional se reserve el derecho a modificar unilateralmente las condiciones de un contrato de duración indeterminada siempre que el profesional esté en la obligación de informar al consumidor con una antelación razonable, y de que éste tenga la facultad de rescindir el

CAPÍTULO SÉPTIMO

que estas mismas consideraciones pudiesen predicarse de todos los contratos celebrados bajo condiciones generales, incluyéndose aquellos suscritos por pequeños empresarios. Consideramos que al proveedor predisponente que contrata con el pequeño empresario empresarios debería exigírsele no solo la anticipación este del contenido de la modificación, sino también la exigencia de que los motivos de la modificación sean razonables y válidos, y que estén especificados en el contrato.

Siguiendo con el marco europeo, respecto de la modificación unilateral del contrato de computación en la nube suscrito por consumidores, debe mencionarse la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos de los contratos de suministro de contenidos digitales. En su considerando 45, se reconoce como una necesidad particular de los contratos de suministro de contenidos digitales la modificación de las características de los contenidos que se suministran a lo largo del tiempo, ya sea por motivos tecnológicos u otras razones. Si bien las modificaciones en favor del consumidor son bienvenidas, pueden existir otras modificaciones que le afecten negativamente, por ejemplo, alterando el equilibrio del contrato o la naturaleza del rendimiento del servicio²³.

Por ello, en su artículo 15, la Propuesta de Directiva establece una serie de condiciones para considerar válida la modificación del contrato de suministro de contenidos digitales (en cuya categoría se incluyen los contratos de computación en la nube). En este artículo se reconoce la facultad del proveedor de servicios de suministro de contenidos digitales de tracto sucesivo para modificar características técnicas que le permitan garantizar la accesibilidad, continuidad y seguridad del servicio y de los contenidos digitales. Si estas modificaciones perjudican el acceso o el uso de los contenidos por el consumidor, será necesario que así lo establezca en el contrato, que se notifique previamente y de manera explícita esta modificación al

contrato".

23 Considerando 45 de 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. "Por motivos tecnológicos o de otro tipo, el proveedor podría verse obligado a modificar las características de los contenidos digitales suministrados durante un periodo de tiempo. Estos cambios suelen ser a favor del consumidor, ya que mejoran los contenidos digitales. En consecuencia, las partes del contrato pueden incluir en el mismo cláusulas que permitan al proveedor realizar modificaciones. Sin embargo, si dichas modificaciones afectan negativamente a la forma en que el consumidor se beneficia de las principales características de funcionamiento de los contenidos digitales, estas podrían alterar el equilibrio del contrato o la naturaleza del rendimiento en virtud del contrato en la medida en que el consumidor puede no haber celebrado dicho contrato. Por tanto, en estos casos las modificaciones deben estar sujetas a determinadas condiciones".

CAPÍTULO SÉPTIMO

consumidor, y que se le permita al consumidor resolver el contrato por disconformidad sin cargos y dándole un plazo razonable para ello, en cuyo caso se le deberá permitir recuperar, en un formato de uso común, los contenidos facilitados al proveedor o los datos generados por el uso del servicio²⁴.

Resultaría conveniente, según nuestro criterio, que estas exigencias al proveedor predisponente pudieran igualmente ser exigidas por los pequeños empresarios suscriptores de estos servicios, en la medida en que se encuentren en una situación de desequilibrio contractual similar a la del consumidor.

En España, el art. 85.3 TRLGDCU declara abusivas "las cláusulas que reserven a favor del empresario facultades de interpretación o modificación unilateral del contrato, salvo, en este último caso, que concurran motivos válidos especificados en el contrato". Por tanto, la declaración de abusividad de la cláusula que reserve al proveedor la facultad de realizar cambios de forma unilateral dependerá, como en los textos normativos anteriormente citados, de la concurrencia de "motivos válidos especificados en el contrato"²⁵. La determinación de la validez

24 Artículo 15 de la Propuesta de Directiva de suministro de contenidos digitales. "Cuando el contrato establezca que los contenidos digitales se suministrarán durante el periodo de tiempo establecido en el contrato, el proveedor podrá modificar su funcionalidad, interoperabilidad y otras características principales de funcionamiento de los contenidos digitales tales como su accesibilidad, continuidad y seguridad, en la medida en que dichas modificaciones afecten negativamente al acceso o al uso de los contenidos digitales por el consumidor, solo si: a) el contrato así lo estipula, b) la modificación se comunica al consumidor con una antelación razonable a través de un medio explícito de notificación en un soporte duradero, c) el consumidor tiene derecho a resolver el contrato sin cargo alguno en un plazo no inferior a 30 días desde la recepción de la notificación, y d) en el momento de la resolución del contrato de conformidad con la letra c), se facilitan al consumidor los medios técnicos para recuperar todos los contenidos previstos de conformidad con el artículo 13, apartado 2, letra c). Si el consumidor resuelve el contrato de conformidad con este artículo, cuando proceda: a) el proveedor reembolsará al consumidor la parte del precio pagado correspondiente al periodo de tiempo tras la modificación de los contenidos digitales, b) el proveedor se abstendrá de utilizar las contraprestaciones no dinerarias que el consumidor haya facilitado a cambio de los contenidos digitales, así como cualesquiera otros datos recogidos por el proveedor en relación con el suministro de los contenidos digitales, incluido cualquier contenido facilitado por el consumidor".

25 El Juzgado de Primera Instancia e Instrucción núm. 5 de Segovia establece, en su sentencia de 20 de junio de 2016, respecto de un contrato entre la compañía Movistar y un consumidor, el carácter abusivo por falta de transparencia de una cláusula predispuesta que permitía al operador modificar las condiciones contractuales por motivos genéricos. Basándose en esta cláusula, del literal "en la cláusula 11 de las condiciones particulares se prevé que "Movistar podrá modificar las presentes condiciones particulares por los siguientes motivos: variaciones de las características técnicas de los equipos o redes, cambios tecnológicos que afecten al producto, variaciones de las condiciones económicas existentes en el momento de la contratación del servicio y evolución del mercado", el operador de telefonía aumentó el precio de la cuota del producto en cinco euros mensuales. Aunque se ofrecía al consumidor la posibilidad de rescindir el contrato sin coste ni penalización, al tener el demandante la condición de consumidor, la sentencia afirma en el Fundamento Segundo que este tiene "derecho a recibir una información precontractual clara y fidedigna en la oferta de productos y

CAPÍTULO SÉPTIMO

de estos motivos dependerá, a nuestro entender, de la naturaleza de los concretos servicios objeto del contrato, de la letra de la propia cláusula, y la interpretación integradora junto con el resto de cláusulas que determina el art. 82.3 del TRLGDCU²⁶. Por tanto, será preferible que el proveedor establezca en la cláusula de modificación unilateral los motivos que puedan considerarse "razones válidas" que motiven la variación, pudiendo relacionarse así con su deber de información precontractual²⁷.

Las regulaciones comunitarias y europeas anteriormente expuestas, deberían poder aplicarse de modo analógico, en nuestra opinión, a contratos suscritos por pequeños empresarios y profesionales que estén en una situación de desequilibrio equiparable a la del consumidor²⁸. Asimismo, deberá estarse a la espera de la

servicios, así como derecho a la protección de sus legítimos intereses económicos y sociales; en particular frente a las prácticas comerciales desleales y la inclusión de cláusulas abusivas en los contratos", de acuerdo con el artículo 8 del Texto Refundido que aprueba la Ley General para la Defensa de Consumidores y Usuarios. Asimismo, afirma en el Fundamento Tercero que "Se trata de motivos tan genéricos y faltos de precisión que resulta imposible a su través que el consumidor pueda conocer por qué y en qué medida se puede producir una modificación del coste del servicio, sobre todo cuando como ocurre en el caso de autos es al alza. En consecuencia, al tratarse de una cláusula poco clara y comprensible, que además está redactada de forma unilateral y general por el operador, podría ser considerada perfectamente como cláusula abusiva por oscuridad y falta de transparencia". Asimismo, afirma la sentencia que "además, esa falta de motivación de la modificación del precio se mantiene en la carta informativa remitida al demandante en el mes de abril de 2015, porque en ella no se concreta la razón que motiva el aumento del precio y por qué se aumenta el precio del producto en cinco euros. Igual que se aumentó en cinco euros, pudo haberse aumentado en dos o en quince, porque no se explica ni el porqué del aumento ni el porqué de la cuantía del aumento. Esto coloca al consumidor en una situación de absoluta indefensión, ya que le limita el derecho a mostrar su disconformidad e impugnar el aumento del precio cuando quiere, como es su derecho, seguir con el contrato y a que éste se cumpla en las condiciones de precio pactadas", de acuerdo con el artículo 1124 del Código Civil. Afirma también que "Esa información,(...), se debe dar al consumidor cuando se le comunica la variación del precio, no cuando éste protesta o impugna, porque entonces la obligatoria información previa acerca de la modificación del coste quedaría vacía de contenido, y la novación objetiva producida con la modificación del precio iría en contra de la norma general del artículo 1256 del Código Civil, en el que se establece que la validez y el cumplimiento de los contratos no puede dejarse al arbitrio de uno de los contratantes".

26 Art. 82.3 del Texto Refundido que aprueba la Ley General para la Defensa de Consumidores y Usuarios y otras leyes complementarias.: "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".

27 *Discussion Paper on Modifications on Cloud Computing Contracts* [en línea], pág. 6. Disponible en: <http://ec.europa.eu/justice/contract/files/expert_groups/modification_contracts_en.pdf>. [Fecha de consulta: 13 de febrero de 2017].

28 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

CAPÍTULO SÉPTIMO

aprobación y, en su caso, futura transposición de la mencionada Propuesta de Directiva de suministro de contenidos digitales.

A nuestro parecer, estas cláusulas de reserva de modificación unilateral del contrato son aceptables e incluso beneficiosas para la evolución del sector, puesto que permiten mayor flexibilidad y adaptabilidad a los vertiginosos avances de la técnica informática y a los eventuales cambios de la legislación aplicable a las relaciones entre proveedor *cloud* y cliente, así como responder a la necesidad de una dinámica respuesta por parte de las empresas para mantener o mejorar la posición en el mercado. Sin embargo, opinamos igualmente que deben ir acompañadas de motivos válidos predeterminados, de los cuales el cliente pequeño empresario debe estar informado, para no situarle en una posición de desamparo, así como de la facultad de resolver el contrato sin cargos ni costes.

2.2.- La comunicación de las modificaciones. El consentimiento implícito por el uso continuado del servicio

La forma más utilizada para dar a conocer las modificaciones de contrato suele ser a través de actualizaciones de la página web del proveedor de servicios *cloud*, y eventualmente, se introducen enlaces a versiones anteriores²⁹. Las condiciones generales del contrato suelen indicar que, cuando el cliente continúa haciendo uso del servicio tras haberse llevado a cabo esa modificación, se está produciendo una aceptación tácita de las nuevas modificaciones³⁰. No obstante,

computación en la nube".

29 Así sucede en muchos de los contratos de adhesión para servicios de computación en la nube, según han observado ciertos autores. BRADSHAW, Simon; MILLARD, Christopher; WALDEN, Ian, *op. cit.*, pág. 51.

30 A continuación, veamos como se recoge lo anterior en una cláusula contractual: "Es posible que cambiemos estas condiciones de vez en cuando debido a los cambios que se realizan en nuestros servicios y las leyes que se aplican a usted y a nosotros. Fecharemos y publicaremos la versión más reciente de estas condiciones en el sitio. Si realizamos algún cambio, se lo notificaremos modificando la fecha de «Última modificación» en la parte superior de estas condiciones y, según sea apropiado, podríamos enviarle un aviso adicional (por ejemplo, añadiendo un comunicado en la página inicial o enviándole una notificación por correo electrónico). Los cambios efectuados empezarán a surtir efecto en el momento de la publicación en los servicios de la versión modificada de estas condiciones (o en otra fecha de entrada en vigor posterior indicada en el encabezamiento de las condiciones modificadas). Si a nuestro juicio las modificaciones de estas condiciones son importantes, se las notificaremos por medio de los servicios o enviándole un mensaje a la dirección de correo electrónico asociada a su cuenta. La notificación de otros cambios podrá realizarse en el sitio o los blogs de box relacionados. Por lo tanto, le instamos a que compruebe la fecha de estas condiciones

CAPÍTULO SÉPTIMO

según el criterio del proveedor y atendiendo a la relevancia del cambio, en ocasiones el proveedor comunica los cambios en las condiciones contractuales al cliente de una manera más directa, por ejemplo, a través de un aviso mediante correo electrónico³¹.

Al continuar haciendo uso del servicio, el cliente puede estar aceptando un cambio en el contrato *cloud*, y, por tanto, puede estar renunciando a la posibilidad de rescindir ese contrato con el proveedor sin tener que sufrir una penalización por cancelación anticipada de los servicios. Por ello, consideramos más que recomendable que, si se permite al proveedor modificar el clausulado unilateralmente, este se comprometa a comunicar al cliente esos cambios de una manera más rigurosa, y permitirle extinguir la relación contractual si está disconforme, especialmente en aquellos servicios destinados a clientes empresariales y/o remunerados. Por su parte, la legislación de protección al consumidor prevé la posible abusividad de este tipo de cláusulas (art. 85.3 TRLGDCU³²)³³.

cada vez que visite el sitio para saber si se han actualizado. Si actualizamos estas condiciones y usted no está de acuerdo con los cambios, deberá decidir libremente si las acepta o deja de utilizar los servicios. Puede desactivar su cuenta en cualquier momento en los ajustes de «su cuenta». Si continúa accediendo a los servicios o usando cualquier parte de los mismos, se entiende que acepta los cambios de las condiciones. Si no acepta alguno de esos cambios, no estamos obligados a seguir proporcionándole los servicios, y debe cancelar los servicios y dejar de usarlos". Como puede deducirse, esta cláusula supone para el cliente una carga adicional: la comprobación periódica de la existencia de cambios en las condiciones del servicio tras su suscripción. Si no se le comunica la existencia de ese cambio a través de un correo electrónico u otro sistema más notorio que una mera actualización en la página web del proveedor, es probable que esta modificación pase desapercibida, con lo cual esté consintiendo implícitamente a las modificaciones efectuadas por el simple hecho de continuar utilizando el servicio. Condiciones del software como servicio Box [en línea]. Disponible en: <<https://www.box.com/es-419/legal/termsofservice>>. [Fecha de consulta: 22 de mayo de 2017].

31 Como ejemplo de lo anterior, el proveedor *cloud* Dropbox vincula la notificación por correo electrónico a cambios que puedan resultar perjudiciales para el cliente, como se afirma en sus condiciones para acuerdos empresariales: "Modificaciones en los Servicios. Dropbox podría actualizar los servicios cada cierto tiempo. Si Dropbox modifica los servicios de forma que reduzca significativamente su funcionalidad, Dropbox informará al cliente a través de la dirección de correo asociada a su cuenta". Acuerdo empresarial de Dropbox [en línea]. Disponible en: <https://www.dropbox.com/es_ES/privacy#business_agreement>. [Fecha de consulta: 13 de febrero de 2017].

32 Art. 85.3 del Texto Refundido que aprueba la Ley General para la Defensa de Consumidores y Usuarios y otras leyes complementarias: "Las cláusulas que vinculen cualquier aspecto del contrato a la voluntad del empresario serán abusivas y, en todo caso, las siguientes: (...) 3. Las cláusulas que reserven a favor del empresario facultades de interpretación o modificación unilateral del contrato, salvo, en este último caso, que concurran motivos válidos especificados en el contrato. (...)".

33 Consideramos que serían recomendables cláusulas similares a la contenida en las condiciones generales de servicios del proveedor español Acens para la mayoría de sus servicios: "Acens se reserva la facultad de modificar unilateralmente la presentación, configuración y operatividad del Servicio,

CAPÍTULO SÉPTIMO

La posibilidad de que el cliente pueda oponerse a esos cambios en las características del servicio de manera individual, y exigir la prestación que desde un inicio llevaba recibiendo, no suele ser factible en la práctica, ya que, al tratarse de servicios que se prestan de manera uniforme y masificada, implican aspectos técnicos complejos que impiden la prestación diferenciada del suministro del servicio entre distintos clientes.

En resumen, consideramos que sí debe permitirse que el proveedor efectúe modificaciones en las condiciones contractuales y en aspectos materiales del servicio, en beneficio del progreso de la técnica y de la mejora y actualización del servicio prestado. Sin embargo, si estas novedades suponen un menoscabo, aunque sea mínimo, en el servicio o en su percepción por el cliente, es deseable que las cláusulas que permiten la modificación unilateral se interpreten de manera restrictiva, y que esos cambios no se hagan efectivos inmediatamente, en la medida de lo posible. Creemos apropiado que se informe al cliente de tales cambios, y que se le ofrezca la oportunidad efectiva de terminar el contrato sin penalización (y, reembolsándole, en su caso, los pagos adelantados que hubieren podido tener lugar), de acuerdo con la buena fe contractual y el deber de diligencia del proveedor. Además, consideramos que sería factible que los proveedores del sector *cloud* utilizasen otros mecanismos que permitieran asegurar el consentimiento informado del cliente en relación a estas modificaciones, especialmente de aquellas que puedan considerarse relevantes o que le perjudiquen de alguna manera, y que se reduzca al mínimo la presunción de que el cliente que continúa en el uso del servicio *cloud* está aceptando los cambios efectuados por el proveedor³⁴.

siempre y cuando dicha modificación no afecte la funcionalidad ni los compromisos del Servicio adquiridos, ni suponga ningún incremento de los precios acordados. Cuando Acens introduzca cualquier modificación que suponga un incremento de los precios acordados o de las condiciones previstas en las presentes CGC [condiciones generales] o las condiciones particulares aplicables al servicio [concreto] procederá a notificar los términos de la modificación y la variación del precio con un (1) mes de antelación a la fecha en que la modificación haya de ser efectiva. En la mencionada notificación, Acens informará al cliente de su derecho a resolver el presente contrato sin penalización en el caso de que no esté conforme con las modificaciones propuestas". Aunque no lo recoja expresamente el texto, entendemos que esta notificación expresa se realizará a través de correo electrónico o un mecanismo similar, y no como una mera actualización en el sitio web del proveedor. Documento disponible en línea. <http://www.acens.com/file_download/condiciones_generales_de_contratacion_electronica_acens.pdf>. [Fecha de consulta: 5 de mayo de 2016].

34 Por ejemplo, la introducción de pestañas o avisos que impidan al cliente continuar con el uso del servicio si no se ha accedido previamente a la información sobre los aspectos que han sufrido modificaciones relevantes para el cliente.

CAPÍTULO SÉPTIMO

Por último, queremos apuntar la existencia de plataformas en línea que, conscientes de la constante reforma de condiciones de uso, políticas de privacidad y otros textos reguladores de la relación proveedor-cliente/usuario de servicios en línea, y de la falta de notificación de muchos de esos cambios, permiten visualizar, vigilar y comparar versiones de los términos y condiciones de proveedores que operan en el tráfico *online*³⁵. Puede ser especialmente útil en aquellos casos en los que el cliente carezca de acceso a anteriores versiones de las cláusulas modificadas o cuando no se le comuniquen eventuales modificaciones de las condiciones generales suscritas.

3.- LA SUSPENSIÓN DEL SERVICIO

En muchas ocasiones, el proveedor de servicios de computación en la nube utiliza una cláusula general para reservarse el derecho a suspender el contrato según crea conveniente. Aunque la redacción de estas cláusulas diferirá de uno a otro proveedor, suelen quedar bajo su criterio los motivos y la procedencia de la suspensión, la existencia de comunicación previa al cliente o de requerimientos para evitar esa interrupción del servicio, así como sus efectos (duración de la interrupción, condiciones para su restauración, posibilidad de recuperación de los datos, etc.).

A continuación, nos detendremos en analizar cada una de estas cuestiones.

3.1.- Las razones de la suspensión del servicio y su validez

En la mayoría de contratos de computación en la nube que se han analizado para la realización de este trabajo, el proveedor ha predispuesto alguna cláusula contractual en la cual queda habilitado para suspender el servicio discrecionalmente.

35 Aplaudimos la iniciativa de la página web *Términos y Condiciones*, fundada por los españoles Jordi Morell y Alberto de Rodrigo, y de su rastreador en línea, que monitoriza los cambios que se producen en más de 7.000 textos legales de proveedores de servicios digitales, permitiendo así que el cliente pueda detectar cambios en los textos legales de los servicios monitorizados que no hayan sido comunicados por el proveedor. Disponible en: <<https://tracker.terminosycondiciones.es/about>>. [Fecha de consulta: 13 de febrero de 2017].

CAPÍTULO SÉPTIMO

En ocasiones, el propio proveedor establece las causas específicas que pueden motivar la suspensión, como el impago, la infracción de las políticas de uso adecuado (PUA) por parte del cliente, el requerimiento por parte de autoridades judiciales o administrativas, la inactividad de la cuenta o eventuales problemas de seguridad³⁶. En otros casos, simplemente se reserva la facultad de suspensión de forma amplia, y sin someterse a la obligación de alegar al cliente causa o motivo alguno³⁷. Se trate de

36 Las Condiciones del software como servicio (SaaS) de almacenamiento remoto *Dropbox Business* contemplan que la suspensión puede tener lugar en caso de infracción contractual, peligro del devengo de responsabilidades, emergencias de seguridad o retraso en las cuotas devengadas: "Suspensión de cuentas de usuario final por parte de Dropbox. Si un usuario final (i) infringe este acuerdo; o (ii) utiliza los servicios de un modo que Dropbox crea de buena fe que provocará responsabilidades, Dropbox podría solicitar al cliente que suspenda o cancele la cuenta de usuario final en cuestión. Si el cliente no suspende o cancela la cuenta de usuario final con la debida diligencia, Dropbox podría hacerlo por iniciativa propia. A pesar de cualquier otra disposición de este acuerdo, si se produce una emergencia de seguridad, Dropbox podría suspender automáticamente el uso de los servicios. Dropbox realizará todos los esfuerzos comercialmente razonables para limitar la suspensión al efecto mínimo necesario para evitar o solucionar la emergencia de seguridad. Por "emergencia de seguridad" se entenderá: (i) un uso de los servicios que altere o pueda alterar los servicios, el uso de los servicios por parte de otros clientes o la infraestructura empleada para proporcionar los servicios; y (ii) el acceso no autorizado a los servicios por parte de terceros. (...) Dropbox podrá suspender o cancelar los servicios si se produce cualquier retraso en el pago". Acuerdo empresarial de *Dropbox* [en línea]. Disponible en: <https://www.dropbox.com/es_ES/privacy#business_agreement>. [Fecha de consulta: 13 de febrero de 2017].

37 Este es el caso de las condiciones generales del software como servicio (SaaS) de almacenamiento remoto *iCloud*, del proveedor Apple. Aunque se trata de una lista abierta y el proveedor reconoce que puede suspenderse el servicio por otras causas, contempla diferentes situaciones que pueden motivar la interrupción del servicio. Como podremos observar, el proveedor solamente en determinadas ocasiones se compromete a requerir previamente al cliente antes de proceder a la suspensión y a devolver los importes satisfechos por adelantado, aunque se exige de cualquier otra responsabilidad: "Apple puede cancelar o suspender inmediatamente y en cualquier momento, bajo determinadas circunstancias y sin notificación previa, toda o parte de su Cuenta o acceso al Servicio. Entre las causas de esta cancelación se incluyen las siguientes: (a) infracciones de este Contrato o de cualquier otra política o directriz a la que se haga referencia aquí o se publique en el Servicio; (b) una solicitud por su parte para la cancelación o terminación de su Cuenta; (c) una solicitud u orden de imposición legal, de un organismo judicial o de otra agencia estatal; (d) si la provisión del Servicio a usted pasa a ser ilegal; (e) problemas técnicos o de seguridad inesperados; (f) su participación en actividades fraudulentas o ilegales; o (g) no pagar las tarifas que deba con relación al Servicio. Apple realizará cancelaciones o suspensiones de este tipo a su entera discreción, y Apple no se responsabiliza ante usted ni ante terceros de los daños que puedan derivarse o surgir como consecuencia de dicha cancelación o suspensión de su Cuenta o del acceso al Servicio. Además, Apple podrá cancelar su Cuenta con previo aviso si (a) su Cuenta ha sido inactiva por un (1) año; o (b) existe una discontinuación general o modificación importante del Servicio o cualquier parte del mismo. Apple realizará cancelaciones o suspensiones de este tipo a su entera discreción, y Apple no se responsabiliza ante usted ni ante terceros de los daños que puedan derivarse o surgir como consecuencia de dicha cancelación o suspensión de su Cuenta y/o del acceso al Servicio, aunque le devolverá, en forma prorrateada, las tarifas o cantidades ya pagadas". Términos y condiciones de *iCloud* [en línea]. Disponible en: <<http://www.apple.com/legal/internet-services/icloud/es/terms.html>>. [Fecha de consulta: 13 de febrero de 2017].

CAPÍTULO SÉPTIMO

un caso u otro, la redacción de estas cláusulas suele conceder bastante margen de maniobra al proveedor sobre la decisión de la continuidad de la prestación.

Consideramos adecuado, de acuerdo con el principio de buena fe contractual, detallar en el contrato los motivos que puedan llevar al proveedor a imposibilitar el acceso a los datos o a proceder a su borrado progresivo, y planteamos que se establezcan procedimientos internos que permitan la notificación previa al suscriptor y la formulación de alegaciones, con un plazo para subsanar la acción motivadora de tal decisión (por ejemplo, un plazo para proceder al pago de períodos vencidos que se adeuden), y la determinación de otro plazo razonable que le permita recuperar la información migrada y evitar su pérdida. Una suspensión del servicio *cloud* en ocasiones puede suponer la paralización de la operativa empresarial del cliente, y, consecuentemente, pueden provocarle perjuicios económicos sin posibilidad alguna de defenderse u obtener compensación³⁸.

38 Cuando los servicios se prestan sin contraprestación económica, el proveedor suele autoconcederse facultades más amplias en cuanto a la suspensión del servicio que si los servicios son de pago, así como exigir al cliente el pago de un importe adicional si pretende recuperar la información migrada. A continuación, la redacción de la cláusula relativa a la suspensión del software como servicio de almacenamiento remoto *Box*, en las condiciones del acuerdo suscrito tanto por empresas como por particulares: "Nos reservamos el derecho a suspender temporalmente o poner fin a su acceso a los Servicios en cualquier momento, a nuestra entera discreción, con o sin previo aviso y sin contraer responsabilidad alguna con respecto a usted por: a) el incumplimiento real o supuesto de estas Condiciones; b) su uso de los Servicios de una manera que podría suponer una responsabilidad legal para Box o interrumpir el uso de los Servicios por parte de otros; c) la sospecha o la detección de código malicioso, virus u otros códigos dañinos introducidos por usted o ubicados en su cuenta; d) tiempo de inactividad no previsto o frecuente; e) uso de demasiada capacidad de almacenamiento o de un ancho de banda excesivo; f) problemas técnicos y cortes imprevistos; o g) si usted ha cesado sus actividades, ha realizado alguna cesión en beneficio de los acreedores o una disposición de activos similar, o se ha convertido en objeto de bancarota, reorganización, liquidación, disolución o un procedimiento similar. En el caso de que, por determinación de Box, la suspensión pudiera ser indefinida o Box haya decidido poner fin a su acceso a los Servicios, Box hará todo lo razonable desde el punto de vista comercial para notificárselo por medio de los Servicios o por correo electrónico a la dirección asociada con su cuenta. También podremos dar por finalizado el contrato por cualquier motivo con un plazo de 30 días de antelación. Usted acepta que si se suspende o se da por terminado su acceso a los Servicios, ya no podrá acceder al Contenido almacenado mediante los Servicios. A la terminación por parte de Box de su acceso a los servicios o su uso de los mismos, por razones distintas a motivo justificado, o por indicación de usted, puede solicitar el acceso a su contenido, que le facilitaremos por un importe adicional. Usted deberá realizar esa solicitud en los cinco (5) días siguientes a la terminación. De lo contrario, el contenido que usted haya almacenado mediante los servicios no se podrá recuperar, y no tendremos ninguna obligación de mantener los datos almacenados en su cuenta". Nos detendremos más adelante en la cuestión de la recuperación de los datos del cliente migrados durante el uso del servicio, cuando debido a la suspensión este se ve privado de acceder a ellos. Condiciones de uso del servicio de almacenamiento remoto de datos Box [en línea]. Disponibles en: <<https://www.box.com/legal/termservice/ES/>>. [Fecha de consulta: 13 de febrero de 2017].

CAPÍTULO SÉPTIMO

La validez de la suspensión se debe valorar, al igual que sucede con la modificación unilateral del servicio, atendiendo a los motivos que fundamenten cada concreta decisión de interrumpir el servicio tomada por el proveedor. Por esta razón, a continuación nos detendremos con más detalle en algunos de los motivos que más frecuentemente motivan la suspensión del servicio de computación en la nube.

3.1.1.- El impago o retraso en el abono de cuotas adeudadas por el cliente *cloud*

Si la razón principal es el impago de las cuotas devengadas por el uso del servicio, de acuerdo con el art. 1124 del Código Civil, el proveedor puede elegir entre exigir el cumplimiento o la resolución del contrato³⁹. En el concreto caso que nos ocupa, puede entenderse la suspensión del servicio como un paso previo a la resolución contractual, que procederá en caso de que el incumplimiento por parte del cliente *cloud* deudor sea definitivo. Del mismo modo, si el cliente no atiende al requerimiento de pago que le efectúe el proveedor, que resulta facultativo de acuerdo con el mencionado artículo del Código Civil, el proveedor podrá resolver el contrato.

Atendiendo a la importancia que la suspensión del contrato puede comportar para la continuidad empresarial de los clientes que utilicen el servicio dentro del ejercicio de su actividad económica, se deberá notificar al cliente de la existencia de ese incumplimiento y darle un plazo para atender a los pagos antes de proceder a la resolución contractual unilateral, en atención a la buena fe contractual.

3.1.2.- El incumplimiento de las políticas de uso adecuado

El uso correcto del servicio obedece a otra de las obligaciones principales del cliente de servicios *cloud*⁴⁰, con lo cual, si el cliente incumple lo acordado en la política de uso del servicio, y realiza actividades ilícitas o prohibidas

39 Art. 1124 del Código Civil: "La facultad de resolver las obligaciones se entiende implícita en las recíprocas, para el caso de que uno de los obligados no cumpliera lo que le incumbe. El perjudicado podrá escoger entre exigir el cumplimiento o la resolución de la obligación, con el resarcimiento de daños y abono de intereses en ambos casos. También podrá pedir la resolución, aun después de haber optado por el cumplimiento, cuando éste resultare imposible".

40 De acuerdo con las obligaciones derivadas de la naturaleza jurídica que, en nuestra opinión, corresponde al contrato de computación en la nube como contrato de servicios. Ver capítulos "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube" y "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

CAPÍTULO SÉPTIMO

contractualmente, el proveedor puede igualmente exigir el cumplimiento de la política o suspender el contrato por llevar a cabo usos prohibidos.

Por los mismos motivos de continuidad empresarial, dentro del deber de buena fe contractual se podría entender implícita la puesta en conocimiento del cliente de su eventual infracción de las condiciones de uso del servicio *cloud* y, si procede, el requerimiento a modificar su conducta, todo ello antes de proceder a la suspensión temporal del servicio o a la terminación definitiva del suministro. Un problema específico a destacar es, como se ha comentado en capítulos anteriores de este trabajo, la discrecionalidad del proveedor a la hora de decidir en qué casos y forma considera que se ha producido una infracción, y la falta de mecanismos a disposición del usuario para realizar alegaciones o manifestar su disconformidad⁴¹.

La suspensión por incumplimiento de las políticas de uso adecuado puede resultar problemática para empresas cliente que suministran servicios a usuarios finales, puesto que el mal uso de los servicios por un usuario final puede poner en jaque la prestación total del servicio a un cliente pequeño empresario. En estos casos, por exigencias del principio de buena fe contractual, es recomendable que se informe al cliente de las actuaciones de usuarios finales que puedan provocar la suspensión del servicio, para que este pueda incluirlo en las cláusulas contractuales que suscriba con los usuarios finales, actuando de mecanismo de información y a la vez de prevención y limitación de responsabilidades en cuanto a daños derivados de un potencial mal uso del servicio.

3.1.3.- Las necesidades técnicas

Otras razones para interrumpir el servicio que se consideran habituales y son mayoritariamente aceptadas por el cliente suscriptor son aquellas motivadas por necesidades técnicas o aquellas que impliquen riesgos para la continuidad o seguridad del servicio⁴². En estos casos, el proveedor deberá actuar diligentemente e informar a sus clientes, en la medida en que le sea posible, de aquellas incidencias relevantes que puedan afectar al uso correcto del servicio o a la seguridad de los

41 Ver apartado "Legalidad y pertinencia 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".

42 KUAN, W. Hon; MILLARD, Christopher; WALDEN, Ian; "*Negotiated Contracts for Cloud Services*", *Cloud Computing Law*, Oxford, 2013, pág. 102.

CAPÍTULO SÉPTIMO

datos alojados remotamente.

Aconsejamos definir o ejemplificar en el contrato de computación en la nube los conceptos de caso fortuito y fuerza mayor, para que recojan una interpretación conforme a la normativa, sean previsibles por el cliente y restrinjan suspensiones o interrupciones del servicio tan amplias como el proveedor en ocasiones pueda pretender, o que oculten infracciones de su deber de diligencia profesional.

3.1.4.- Otras causas

Si de la redacción del contrato puede extraerse que el proveedor se ampara en una decisión arbitraria para suspender el servicio⁴³, la cláusula general que lo establece sería susceptible de considerarse inválida de acuerdo al artículo 1256 del Código Civil⁴⁴, y abusiva bajo la normativa de protección al consumidor⁴⁵.

Del mismo modo, los contratos que prevean otras causas de suspensión del servicio podrán someterse a una interpretación global y a un juicio de valor cuando el proveedor cese en la prestación del servicio a uno o múltiples clientes (por ejemplo, en casos de concurso de acreedores del proveedor o suscriptor, por motivos comerciales, etc.), ya que se pueden originar responsabilidades para el proveedor en relación a eventuales daños sufridos por clientes empresarios o usuarios finales⁴⁶.

43 Por ejemplo, una cláusula que permita al proveedor suspender o cancelar en cualquier momento servicios prestados de forma gratuita. En nuestra opinión, el hecho de que un servicio se preste sin contraprestación económica no habilita en ningún modo al proveedor para poder cancelar o suspender el servicio de forma arbitraria, pues, como se ha observado en capítulos anteriores, el cliente asume, con el contrato, cargas o deberes de naturaleza no económica.

44 Art. 1256 del Código Civil: "La validez y el cumplimiento de los contratos no pueden dejarse al arbitrio de uno de los contratantes".

45 Art. 82.4 de la TRLGDCU: "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 (...), e) resulten desproporcionadas en relación con el perfeccionamiento y ejecución del contrato". 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*".

46 Dado que en el *Outsourcing* informático las modificaciones entre las partes son especialmente relevantes, puesto que se trata de un contrato *intuitu personae*, es frecuente que en los acuerdos que regulan esta relación jurídica se hallen pactos expresos de la imposibilidad de que el proveedor ceda el contrato a un tercero sin el consentimiento del cliente. En cambio, el *Cloud Computing* de implementación pública, a diferencia del *Outsourcing*, es un contrato predispuesto para una multitud de potenciales clientes, con lo cual el proveedor puede utilizar una cláusula de modificación unilateral para introducir cambios subjetivos en el contrato. Respecto del

CAPÍTULO SÉPTIMO

Finalmente, una vez expuestos los casos de suspensión, acabamos señalando que la Propuesta de Directiva de suministro de contenidos digitales establece la falta de continuidad adecuada del suministro de contenidos digitales como un incumplimiento de una de sus obligaciones principales, y como tal, cuando tal interrupción sea significativa y no se resuelva en un breve período de tiempo, el consumidor quedaría habilitado para resolver el contrato⁴⁷.

3.2.- El procedimiento de suspensión unilateral

Como hemos puesto de relieve, el procedimiento mediante el cual el proveedor comunicará y valorará las diferentes circunstancias que provoquen una concreta suspensión del servicio no es en ningún modo uniforme. En primer lugar, porque es denominador común en los contratos que se han examinado en la elaboración de este trabajo la no inclusión de detalles sobre este tipo de procedimientos de decisión y valoración de las causas que motivan una suspensión, así como de la oportunidad del cliente afectado de realizar alegaciones o de permanecer informado sobre el curso de la investigación interna que pueda llevarse a cabo⁴⁸. Aunque en la mayoría de contratos el proveedor se comprometa a comunicar

Outsourcing informático, nos remitimos a APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática. Introducción al outsourcing de los sistemas de información*, Granada, 2002, pág.151.

47 Así lo recoge su considerando 35 ("El incumplimiento del proveedor de suministrar contenidos digitales al consumidor de conformidad con el contrato constituye un incumplimiento grave de la principal obligación contractual del proveedor, que debe permitir que el consumidor resuelva el contrato de forma inmediata. Si el proveedor no ha incumplido inicialmente el suministro de contenidos digitales, las interrupciones del suministro que causen que los contenidos digitales no estén disponibles o accesibles para el consumidor en un breve periodo de tiempo deben tratarse como una no conformidad con el contrato, y no como un incumplimiento en el suministro. En particular, el requisito de la continuidad adecuada de los contenidos digitales también debe cubrir más que las interrupciones por un corto periodo de tiempo insignificante del suministro") y sus artículos 6.1 ("Para estar en conformidad con el contrato, los contenidos digitales serán, cuando proceda: a) en la cantidad, con la calidad, duración y versión, y poseerán la funcionalidad, interoperabilidad y demás características de funcionamiento tales como accesibilidad, continuidad y seguridad, según venga requerido por el contrato, incluyendo cualquier información precontractual que forme parte integrante del contrato, (...)") y 12.5 ("El consumidor puede resolver el contrato solo si la falta de conformidad con el mismo impide su funcionalidad, interoperabilidad y otras características principales de funcionamiento de los contenidos digitales, tales como su accesibilidad, continuidad y seguridad previstas en el artículo 6, apartados 1 y 2. La carga de la prueba de que la falta de conformidad con el contrato de los contenidos digitales no impide su funcionalidad, interoperabilidad y otras características principales de funcionamiento de los contenidos digitales corresponderá al proveedor").

48 A modo de ilustración, el proveedor Box facilita esta información sobre el procedimiento de suspensión del servicio: "En el caso de que, por determinación de Box, la suspensión pudiera ser indefinida

CAPÍTULO SÉPTIMO

al cliente las suspensiones del servicio, lo cierto es que en otras ocasiones no se comprometen a avisar previamente al cliente afectado, o se reservan el derecho a interrumpir el servicio sin notificación⁴⁹. Igualmente, el hecho de que no se contemple en el contrato esta notificación previa no implica que en la práctica no se realicen tales avisos.

De lo anterior puede extraerse que en los contratos predispuestos de servicios computación en la nube nos encontramos, por un lugar, con una clara falta de uniformidad sobre el compromiso del proveedor en cuanto a efectuar notificaciones al cliente en casos de suspensión del servicio; y, por otra, una falta de transparencia en cuanto al procedimiento interno de valoración de las causas que motiven esa interrupción.

Se ha mencionado anteriormente que la suspensión sin previo aviso de un servicio de computación en la nube puede suponer para el cliente, sobre todo si es un pequeño empresario, serios inconvenientes en el ejercicio de su actividad económica. Por ello, creemos que es importante la existencia de un aviso previo cuando el proveedor tenga la intención de, unilateralmente, suspender el servicio de uno o más clientes. Por otra parte, consideramos que los proveedores deberían establecer mecanismos de información más transparentes y garantistas con el cliente, para que estos puedan conocer el estado del procedimiento, efectuar alegaciones cuando sea procedente, y prever el tiempo durante el cual el acceso al servicio no será posible. Todo ello fundamentado en el principio de buena fe contractual y en el deber de diligencia profesional.

Como mejora recomendable, proponemos la inclusión en el contrato de un

o Box haya decidido poner fin a su acceso a los Servicios, Box hará todo lo razonable desde el punto de vista comercial para notificárselo por medio de los Servicios o por correo electrónico a la dirección asociada con su cuenta. También podremos dar por finalizado el Contrato por cualquier motivo con un plazo de 30 días de antelación". El único indicio sobre el procedimiento que tendrá lugar en caso de suspensión es la posibilidad (pero no el compromiso) de que sea notificado al cliente a través de la dirección de correo electrónico facilitada por el cliente a tal efecto. En esta cláusula se contempla, además, la posibilidad de suspender el servicio por cualquier motivo a discreción del proveedor, comprometiéndose con un preaviso de 30 días, y la posibilidad de que puedan dictaminarse suspensiones por tiempo indefinido. Condiciones del servicio *Box* [en línea]. Disponible en: <<https://www.box.com/legal/termsofservice/ES/>>. [Fecha de consulta: 13 de febrero de 2017].

⁴⁹ Se ha observado, en la comparativa entre servicios *cloud* de diferentes proveedores llevada a cabo durante este estudio, que las notificaciones previas a interrupciones relevantes del servicio son la tónica dominante en la práctica comercial habitual, aunque se hayan reservado el derecho a suspender el servicio sin notificación.

CAPÍTULO SÉPTIMO

listado de posibles causas que habiliten al proveedor pueda suspender la prestación, así como establecer un procedimiento de avisos, plazos para corregir posibles incumplimientos, y una comunicación más eficaz entre las partes. De este modo se equilibraría la posición del cliente, posibilitando la defensa de sus intereses, e igualmente se aumentaría la confianza en el servicio, al facilitar al cliente una información transparente sobre los riesgos de contratar el servicio y sobre sus responsabilidades como usuario.

3.3.- Las consecuencias de la suspensión del servicio para el cliente

De la suspensión del servicio de computación en la nube pueden derivarse diferentes consecuencias para el cliente. La principal consecuencia (en principio, temporal) de la suspensión del servicio y, en su caso, de la posterior terminación, es la falta de disponibilidad del servicio (esto es, el acceso limitado a la plataforma del proveedor que permite al cliente disfrutar de las funcionalidades del servicio, ya sean estas de infraestructura o plataforma, ya sea el uso de una aplicación informática) y, consecuentemente, la imposibilidad de acceso a los datos almacenados en los sistemas del proveedor y accesibles remotamente desde el dispositivo del cliente⁵⁰. Ambos resultados, dependiendo del grado de implementación en la infraestructura de la empresa cliente, pueden suponer la paralización de su actividad empresarial, y, por ello, emergerán consecuencias de índole económica.

Ya hemos señalado que en los contratos predispuestos de computación en la nube, el proveedor intentará limitar al máximo la responsabilidad por daños, con lo cual deberemos acudir al conjunto del contrato para comprobar si, efectivamente, se han suscrito por el cliente empresario cláusulas de aceptación del servicio "tal y como está" o de un alcance exoneratorio similar. De ser así, debemos tener presentes los distintos efectos de la suscripción de estos contratos por parte de empresas y profesionales, y la realizada por consumidores, puesto que los primeros, al haber

50 En esta cláusula del software como servicio de almacenamiento remoto de *iCloud* de Apple se contemplan los efectos de una potencial cancelación de cuenta del cliente: "Si se cancela su cuenta, podría perder todo acceso al servicio y a cualquier parte del mismo, incluidos, sin carácter limitativo, su cuenta, Apple ID, la cuenta de correo electrónico y el contenido. Además, después de un período de tiempo, Apple eliminará la información y los datos almacenados en o como parte de su(s) cuenta(s). (...)". Términos del servicio *iCloud* [en línea]. Disponible en: <<http://www.apple.com/legal/internet-services/icloud/la/terms.html>>. [Fecha de consulta: 13 de febrero de 2017]

CAPÍTULO SÉPTIMO

aceptado exenciones de responsabilidad y, por ende, la renuncia a ser compensados por daños causados por una acción u omisión del proveedor (en este caso, la falta de acceso al servicio y a los datos almacenados), deberán acudir a los tribunales con la pretensión de la declaración de la nulidad de tales cláusulas, puesto que se les presumen válidas al actuar en el marco de su actividad profesional (siéndole exigible, por tanto, el deber de diligencia) y en ejercicio de la autonomía de la voluntad al contratar. Por todo ello, deberá acudir a la aplicación de los artículos⁵¹ 1255⁵², 1256 y 1911 del Código Civil⁵³.

En cuanto a la falta de acceso temporal a los datos que el cliente pueda tener almacenados en los servidores del proveedor y su posibilidad de recuperación, resulta una consecuencia directa de la falta de acceso al servicio, con lo cual, al impedírsele al cliente o usuario entrar en su cuenta, este no tiene posibilidad de recuperar los datos que estén almacenados en los sistemas del proveedor. En cuanto a la reclamación de compensaciones por tal imposibilidad, sucederá lo mismo que con la falta de acceso: si el pequeño empresario ha suscrito limitaciones de responsabilidad que excluyan su derecho a ser indemnizado, difícilmente se harán efectivas tales compensaciones, independientemente de que el pequeño empresario deba responder ante terceros (por ejemplo ante sus propios clientes, como usuarios finales o titulares de derechos sobre los datos migrados). Si el servicio finalmente no llega a restaurarse de nuevo, deberá ofrecerse al cliente la recuperación de esos datos, como parte de las obligaciones inherentes a la naturaleza del contrato *cloud* que incluya el almacenamiento remoto de información y procederse a su posterior

51 Afirma BELLO que "en el ámbito contractual, han de ser estimadas nulas, en principio, todas las convenciones que supongan o impliquen la exoneración total de responsabilidad del deudor, no ya sólo en virtud de lo dispuesto en el art. 1911 CC ["Del cumplimiento de las obligaciones responde el deudor con sus todos sus bienes, presentes y futuros"] sino, más claramente, porque el art. 1256 del mismo cuerpo legal ["La validez y el cumplimiento de los contratos no puede dejarse en manos de uno de los contratantes"] prohíbe que quede al arbitrio de una de las partes cumplir o no cumplir sus obligaciones". El autor refuerza este argumento con las sentencias STS de 4 de julio de 1953 y la Sentencia de la Audiencia Provincial de Barcelona, Sección 16, de 15 de noviembre de 1990. BELLO JANEIRO, Domingo: "Cláusulas de exclusión o reducción de responsabilidad en la Ley General de Consumidores y Usuarios", *Anuario da Facultade de Dereito da Universidade da Coruña*, núm. 2, 1998, págs. 627 a 664.

52 Art. 1255 del Código Civil: "Los contratantes pueden establecer los pactos, cláusulas y condiciones que tengan por convenientes, siempre que no sean contrarios a las leyes, a la moral y al orden público".

53 Esta y otras consideraciones sobre las limitaciones y exoneraciones de responsabilidad contractual se han expuesto con más detalle 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*")" del capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

CAPÍTULO SÉPTIMO

borrado de los sistemas del proveedor, como veremos en apartados posteriores de este mismo capítulo.

Con todo ello, llegado el momento en el cual el proveedor decida cancelar definitivamente el servicio al cliente, consideramos que debería posibilitarse la recuperación de los datos migrados dentro de un plazo razonable, porque el cliente es su titular, y el proveedor no puede privarle de ellos por la mera inclusión de una cláusula contractual que así le habilite y que, además, no ha sido negociada. Más aún, si se trata de datos que puedan tener valor comercial, (secretos de empresa o susceptibles de generar derechos de propiedad intelectual), o que sean de carácter personal⁵⁴.

Como recapitulación, podemos afirmar que la cláusula de suspensión unilateral del contrato debería interpretarse siempre de manera restrictiva, puesto que puede provocar un grave impacto sobre la operativa y continuidad de las empresas usuarias. Además, es una cláusula susceptible de considerarse inválida por vincular el contrato a la voluntad de la parte que predispone las condiciones contractuales (artículo 1256 del Código Civil⁵⁵ y 82.4 del TRLGDCU⁵⁶).

4.- LA EXTINCIÓN DEL CONTRATO

Como hemos observado, uno de los rasgos que caracterizan a la generalidad de los contratos de computación en la nube es su prestación continuada. Estos contratos permanecerán vigentes, en principio, hasta que una de las partes decida no continuar con la relación obligatoria. Igualmente, ante la diversidad de contratos y capacidades suministradas, no es extraño que existan contratos que puedan tener inicialmente una duración determinada, con lo cual la relación, cuando se haya

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

55 Art. 1256 del Código Civil: "La validez y el cumplimiento de los contratos no pueden dejarse al arbitrio de uno de los contratantes".

56 Art. 82.4 de la TRLGDCU: "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 (...), e) resulten desproporcionadas en relación con el perfeccionamiento y ejecución del contrato". 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 computación en la nube".

CAPÍTULO SÉPTIMO

acabado el término de vigencia y dependiendo de lo que el cliente decida, se extinguirá una vez transcurrido el tiempo acordado, se irá renovando de manera automática o se producirá una novación hacia otro contenido obligacional⁵⁷.

En las condiciones generales se recogerán las causas que pueden motivar la terminación del contrato. También contemplarán sus efectos, como las eventuales penalizaciones por cancelación anticipada, la devolución de los pagos adelantados y el procedimiento para que los datos puedan ser recuperados por el cliente y posteriormente eliminados del sistema del proveedor.

Aunque existen importantes aspectos comunes entre los contratos de diferentes servicios de computación en la nube, lo cierto es que los protocolos llevados a cabo una vez terminado el contrato dependerán en gran medida de la política comercial de cada uno de los proveedores. No cabe duda, no obstante, que tras extinguirse un contrato, pueden subsistir otras obligaciones remanentes de la

57 Para esclarecer las diferentes opciones que puede tener el cliente a la hora de contratar un servicio *cloud*, traemos a colación las condiciones generales del servicio *G-Suite para empresas*, del proveedor Google, que permiten la elección entre diferentes opciones de contrato: la primera, el denominado "plan flexible", que implica un contrato de duración indeterminada con pagos mensuales que tendrán lugar indefinidamente hasta que se cancele el servicio, y el "plan anual", que tiene una duración de un año, y que, al finalizar este período, se convertirá de manera automática en un "plan flexible", excepto que el cliente, en su panel de administración, prefiera renovar el contrato con una duración anual. Condiciones generales de *G-Suite* [en línea]. Disponibles en: <https://gsuite.google.com/intl/es/terms/2013/1/premier_terms.html>. [Fecha de consulta: 15 de febrero de 2017]. Igualmente, puede suceder en los contratos de prueba del servicio, o en aquellos casos en los que el cliente decida acceder a servicios más completos, con lo cual el contrato anterior no quedaría exactamente extinguido, sino que es invalidado por unas nuevas condiciones que contemplan específicamente esas cuentas "premium" o con privilegios. Para ilustrar las diferentes concepciones de la duración del contrato *cloud* como contrato de tracto sucesivo, veamos la previsión contemplada en las condiciones generales del proveedor Acens en cuanto a la duración del contrato: "Salvo indicación en sentido contrario en las condiciones particulares y las correspondientes órdenes de pedido, la relación contractual entre Acens y el cliente entrará en vigor el mismo día en el que Acens comunique al cliente la aceptación de la contratación o desde que Acens proceda a la activación del servicio contratado, sea cuál sea el primero en tener lugar. Asimismo, tendrá la duración inicial definida por el cliente en el momento de la activación y solicitud de servicio. Finalizado el período de duración inicial, el servicio se entenderá automática y tácitamente prorrogado por períodos sucesivos equivalentes al periodo de duración inicial contratado, salvo que se resuelva el contrato según los términos indicados en la cláusula 7.2 (Terminación) o se solicite la baja según los términos indicados en la cláusula 7.3 (Preaviso). Sin perjuicio de lo anterior, el cliente que desee migrar el servicio contratado a un plan de contratación de nivel superior podrá realizarlo en cualquier momento, bastando al efecto la mera comunicación en tal sentido a Acens, de conformidad con lo establecido en la cláusula 14". Condiciones generales de la contratación electrónica de servicios Acens [en línea]. Disponibles en: <http://www.acens.com/file_download/condiciones_generales_de_contratacion_electronica_acens.pdf>. [Fecha de consulta: 15 de febrero de 2017].

CAPÍTULO SÉPTIMO

relación jurídica que ha finalizado. En particular, al extinguirse el contrato de servicios de computación en la nube, generalmente deberá procederse a la restitución de los datos al cliente y al borrado de estos datos de los sistemas del proveedor⁵⁸.

Seguidamente nos detendremos en las principales razones que pueden motivar la terminación del contrato por una de las partes y la posterior extinción de la relación contractual. Acabaremos este capítulo examinando los principales efectos de la extinción de la relación entre las partes del contrato *cloud*: la posibilidad de recuperar los datos, durante un plazo de tiempo razonable, en un formato utilizable y que permita transmitirlos a la nube de otro proveedor (o portabilidad de datos); y el borrado definitivo de los datos remanentes en el sistema del proveedor⁵⁹.

4.1.- Las causas de terminación del contrato de computación en la nube en las cláusulas resolutorias

Según hemos comentado, al tratarse de contratos de tracto sucesivo, generalmente se elude en las condiciones generales el establecimiento de un plazo de tiempo durante el cual el contrato se entiende vigente, y en su lugar se establecen causas y condiciones que permitan a las partes extinguir la relación jurídica⁶⁰. De hecho, en contratos suscritos por consumidores, la información sobre la posibilidad de terminar un contrato suscrito inicialmente sin una duración determinada, como sucede generalmente con los contratos de computación en la nube, se constituye por

58 DIEZ-PICAZO, Fundamentos del Derecho Civil Patrimonial, Vol. II. Las relaciones obligatorias, pág. 1085.

59 BRADSHAW, S; MILLARD, C; WALDEN, I, “Standard contracts for Cloud Services” en *Cloud Computing Law*, (coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 52.

60 La duración indefinida (o, en su caso, la renovación automática) de los contratos de computación en la nube supone otra diferencia más con los servicios de *Outsourcing*, puesto que, como afirma APARICIO VAQUERO, la posibilidad de renegociación y valoración de costes de mantenimiento de la relación jurídica y transición a otro proveedor, junto con la incertidumbre que supondría admitir la denuncia sin justa causa en contratos indefinidos motivan que el *Outsourcing* informático se sujete a una contratación por duración determinada. Esta duración oscila, según el autor, desde 2 a 10 años, dependiendo de la política empresarial de las partes contratantes. En relación al *Otusourcing* informático, APARICIO VAQUERO, *La nueva contratación...*, *op. cit.*, pág. 153.

CAPÍTULO SÉPTIMO

imperativo legal en una obligación para el proveedor de servicios *cloud*⁶¹. Cuando el contrato haya sido suscrito por un pequeño empresario, este deber de información sobre las causas de la extinción del contrato se basará en la colaboración mutua y el principio de buena fe contractual. En defecto de pacto, se interpretará el contrato y se podrá acudir a lo regulado a tal efecto en la normativa que subsidiariamente sea de aplicación⁶².

A continuación, comentaremos las causas de terminación de contratos *cloud* que con más frecuencia se establecen en la práctica contractual.

4.1.1.- El desistimiento unilateral

El contrato de computación en la nube a menudo faculta a ambas partes para que puedan terminar la relación obligatoria, aunque de esa decisión probablemente se deriven diferentes consecuencias jurídicas, dependiendo de la parte que efectúe la denuncia, del concreto contenido del clausulado y de la razón que motive el desistimiento.

Cuando sea el cliente quien estime conveniente terminar el contrato de computación en la nube sin que haya mediado incumplimiento por parte del prestador del servicio *cloud*, deberá comunicar su intención al proveedor según lo

61 Así lo establece el art.62.4 del Texto Refundido para la Ley General de Defensa de los Consumidores y Usuarios y otras leyes complementarias: "Los contratos de prestación de servicios o suministro de productos de tracto sucesivo o continuado deberán contemplar expresamente el procedimiento a través del cual el consumidor y usuario puede ejercer su derecho a poner fin al contrato".

62 El acuerdo del software como servicio (SaaS) de almacenamiento remoto *Dropbox para empresas*, aunque recoge expresamente la posibilidad de cancelación del contrato por el cliente ("este acuerdo permanecerá vigente hasta que termine o se cancele la suscripción del cliente a los servicios, o bien hasta que finalice el acuerdo"), únicamente detalla el preaviso y los efectos de la cancelación del acuerdo cuando tenga lugar un incumplimiento contractual o aparezcan problemas con la solvencia o continuidad empresarial de cualquiera de las partes contratantes ("tanto Dropbox como el cliente podrán cancelar el acuerdo si: (i) la otra parte incumple formalmente el acuerdo y no solventa tal incumplimiento en un plazo de 30 días a partir de que se le comunique por escrito; o (ii) la otra parte cesa en su actividad comercial o se somete a un procedimiento de bancarrota no resuelto en menos 90 días. Efectos de la cancelación. En caso de cancelación de este Acuerdo: (i) los derechos otorgados al cliente por parte de Dropbox se extinguirán de inmediato (excepto por lo establecido en esta sección); (ii) Dropbox proporcionará al cliente acceso a su cuenta a las tarifas vigentes en ese momento para que el cliente pueda exportar sus Datos almacenados; y (iii) tras un periodo de tiempo comercialmente razonable, Dropbox podría eliminar los datos almacenados de la cuenta del cliente. Las siguientes secciones sobrevivirán a la cancelación o caducidad de este acuerdo: (...)"). Condiciones generales de *Dropbox para empresas* [en línea]. <https://www.dropbox.com/es_ES/privacy#business_agreement>. [Fecha de consulta: 15 de febrero de 2017].

CAPÍTULO SÉPTIMO

que haya dispuesto este en las condiciones generales⁶³. Las consecuencias de la cancelación de una cuenta pueden variar dependiendo de lo establecido contractualmente, aunque a menudo implicarán una penalización que podría consistir en el desembolso equivalente al importe de una o varias cuotas⁶⁴.

Si el coste de la terminación del contrato para el cliente resulta desproporcionado, puede implicar *de facto* una obligación de permanencia y, aunque el consumidor puede denunciar la abusividad de esta cláusula (art. 62.3 TRLGDCU), el cliente *cloud* que sea empresario en principio deberá asumir tales gastos si quiere extinguir la relación jurídica⁶⁵.

Por el contrario, hemos visto en el apartado anterior que, en ocasiones, el proveedor se reserva el derecho a cancelar el servicio sin necesidad de preaviso. Estas cláusulas son desproporcionadas, porque suponen un desequilibrio entre las partes sin motivación alguna, y pueden calificarse como abusivas en contratos con consumidores⁶⁶. Algunas de las causas de la cancelación del servicio coinciden con

63 Algunos proveedores como Google, Microsoft o Acens ponen a disposición del cliente paneles de control o plataformas para permitirle cancelar en línea los servicios contratados, tal y como contemplan su sitio web o sus condiciones generales. [Fecha de consulta: 17 de febrero de 2017]

64 En ocasiones, el proveedor prevé la compensación por ciertos costes derivados de los servicios prestados al cliente, con lo cual exige el pago de una penalización por cancelación anticipada en aquellos casos en los que se haya podido pactar una permanencia en el servicio. Como ejemplo, esta condición general prevista por el proveedor Acens: "Los servicios prestados por Acens al cliente conllevan para Acens la realización de inversiones y la necesidad de tener costes comprometidos frente a terceros. En consecuencia, en caso de que el cliente dé por finalizado el contrato incumpliendo el periodo mínimo de permanencia o la duración indicada en las condiciones particulares de contratación y sin hallarse cubierto por ninguna de las causas expresadas en los apartados (a) y (b) de la cláusula anterior (terminación del contrato), éste estará obligado, en concepto de indemnización o por cancelación anticipada, a (i) abonar a Acens el precio pactado de los servicios, es decir, las cuotas restantes hasta la finalización del periodo mínimo de permanencia que habrían sido abonadas por el cliente en caso de no haber instado la cancelación anticipada y; (ii) reembolsar a Acens cualquier bonificación o descuento del que se hubiese podido beneficiar a la firma del contrato".

65 Art. 62.3 del Texto Refundido para la Ley General de Defensa de los Consumidores y Usuarios y otras leyes complementarias: "En particular, en los contratos de prestación de servicios o suministro de productos de tracto sucesivo o continuado se prohíben las cláusulas que establezcan plazos de duración excesiva o limitaciones que excluyan u obstaculicen el derecho del consumidor y usuario a poner fin al contrato. El consumidor y usuario podrá ejercer su derecho a poner fin al contrato en la misma forma en que lo celebró, sin ningún tipo de sanción o de cargas onerosas o desproporcionadas, tales como la pérdida de las cantidades abonadas por adelantado, el abono de cantidades por servicios no prestados efectivamente, la ejecución unilateral de las cláusulas penales que se hubieran fijado contractualmente o la fijación de indemnizaciones que no se correspondan con los daños efectivamente causados".

66 Art. 85.4 del Texto Refundido para la Ley General de Defensa de los Consumidores y Usuarios y otras leyes complementarias: "Las cláusulas que vinculen cualquier aspecto del contrato a la voluntad del empresario serán abusivas y, en todo caso, las siguientes: (...) Las cláusulas que autoricen al empresario a (...),

CAPÍTULO SÉPTIMO

los motivos de suspensión del servicio, ya que esta suspensión puede, en ocasiones, desembocar en la extinción del contrato, como sucede, por ejemplo, cuando la cuenta del cliente permanezca inactiva durante un periodo de tiempo previsto contractualmente.

En aquellos casos en los que el proveedor decida cancelar el servicio, es importante que avise con antelación al cliente, para permitirle así obtener nuevas fuentes que le puedan suministrar capacidades similares (otros proveedores de *cloud* o de otros servicios informáticos, o la instalación de elementos hardware que suministren tales capacidades), puesto que de estas capacidades puede depender parte de su actividad empresarial. De la valoración de estas circunstancias dependerá que se entienda que se le ha otorgado al cliente un tiempo "razonable"⁶⁷. Y aunque, como afirman los expertos, no es frecuente que los proveedores en la nube terminen contratos con consumidores y pequeños empresarios sin producirse por parte de aquellos un incumplimiento contractual, no puede descartarse esta hipótesis al entrar en juego intereses comerciales⁶⁸.

Dicho lo anterior, es remarcable que, según la Propuesta de Directiva de suministro de contenidos digitales, el consumidor tendría derecho a resolver el contrato *cloud* cuando lo notifique con antelación al proveedor a través de cualquier medio (art. 13.1⁶⁹), en el caso de que el proveedor incumpla en el suministro de los contenidos (art. 11⁷⁰) o los contenidos suministrados impidan su funcionalidad,

o las que le faculden a resolver los contratos de duración indefinida en un plazo desproporcionadamente breve o sin previa notificación con antelación razonable. Lo previsto en este párrafo no afecta a las cláusulas en las que se prevea la resolución del contrato por incumplimiento o por motivos graves, ajenos a la voluntad de las partes, que alteren las circunstancias que motivaron la celebración del contrato".

67 En la consideración de una cláusula como abusiva, establece el art. 85.4 del Texto Refundido para la Ley General de Defensa de los Consumidores y Usuarios y otras leyes complementarias utiliza este impreciso vocablo, "razonable", para valorar la abusividad de cláusulas con plazos de preaviso demasiado breves: "las que le faculden a resolver los contratos de duración indefinida en un plazo desproporcionadamente breve o sin previa notificación con antelación razonable".

68 Así lo pusieron de relieve el grupo de expertos en contratos de computación en la nube de la *Cloud Computing Strategy* de la Comisión Europea, en su reunión de 9 y 10 de abril de 2014. [En línea]. Disponible en: <http://ec.europa.eu/justice/contract/files/910_april_final_synthesis_en.pdf>. [Fecha de consulta: 15 de febrero de 2017].

69 Artículo 13.1 de la Propuesta de Directiva de Suministro de Contenidos Digitales: "El consumidor ejercerá el derecho a resolver el contrato mediante notificación al proveedor comunicada por cualquier medio".

70 Artículo 11 de la Propuesta de Directiva de Suministro de Contenidos Digitales: "Cuando el proveedor haya incumplido en el suministro de los contenidos digitales de conformidad con el artículo 5, el

CAPÍTULO SÉPTIMO

interoperabilidad u otras características como la accesibilidad, la continuidad o la seguridad del servicio de suministro (art. 12.4⁷¹). En este caso, el proveedor deberá reembolsar los importes adelantados sin demora, se abstendrá de utilizar la información facilitada por el consumidor a modo de contraprestación no dineraria u otros contenidos facilitados (excepto contenidos generados conjuntamente con otros usuarios que sigan de alta en el servicio), le permitirá recuperar los contenidos que ha facilitado por el uso del servicio y que el proveedor retenga. El proveedor, a su vez podría impedir el uso del servicio por el consumidor, por ejemplo, inhabilitando su cuenta de acceso (art. 13.3⁷²).

También se reconoce el derecho del consumidor a resolver contratos de suministros digitales que, como a menudo sucede con los contratos de computación en la nube, son de larga duración, en concreto aquellos contratos cuya duración inicial o cualquier combinación de periodos de renovación exceda de 12 meses, una vez expirado el primer periodo de 12 meses (art. 16⁷³).

4.1.2.- La resolución del contrato por incumplimiento de una de las partes

En la mayoría de los contratos de computación en la nube existen cláusulas que regulan la terminación del contrato motivada por el incumplimiento de las partes⁷⁴.

consumidor tendrá derecho a resolver el contrato inmediatamente en virtud del artículo 13".

- 71 Artículo 12.4 de la Propuesta de Directiva de Suministro de Contenidos Digitales: "El consumidor puede resolver el contrato solo si la falta de conformidad con el mismo impide su funcionalidad, interoperabilidad y otras características principales de funcionamiento de los contenidos digitales, tales como su accesibilidad, continuidad y seguridad previstas en el artículo 6, apartados 1 y 2. La carga de la prueba de que la falta de conformidad con el contrato de los contenidos digitales no impide su funcionalidad, interoperabilidad y otras características principales de funcionamiento de los contenidos digitales corresponderá al proveedor".
- 72 Artículo 13.3 de la Propuesta de Directiva de Suministro de Contenidos Digitales: "En el momento de resolución, el proveedor podrá impedir cualquier otro uso de los contenidos digitales por el consumidor, en particular haciendo que los contenidos digitales no sean accesibles para el consumidor o inhabilitando la cuenta de usuario del consumidor, sin perjuicio del apartado 2, letra c)".
- 73 Artículo 16.1 de la Propuesta de Directiva de Suministro de Contenidos Digitales: "Cuando el contrato prevea el suministro de contenidos digitales durante un periodo de tiempo indeterminado o cuando la duración inicial del contrato o cualquier combinación de periodos de renovación exceda de 12 meses, el consumidor tendrá derecho a resolver el contrato en cualquier momento tras la expiración del primer periodo de 12 meses".
- 74 Veamos un ejemplo de cómo se contempla en unas condiciones generales, y cómo se refleja la necesidad de que el incumplimiento que permita fundamentar la resolución del contrato sea sustancial, para que pueda fundamentar la resolución del contrato, y suele reflejarse de modo similar en la letra de otros muchos contratos de computación en la nube: "Rescisión por

CAPÍTULO SÉPTIMO

El incumplimiento contractual permite resolver el contrato vigente de computación en la nube, cuando la parte perjudicada así lo decida (art. 1124 del Código Civil⁷⁵). Sin embargo, tal y como han interpretado reiteradamente la jurisprudencia y la doctrina, no será suficiente cualquier incumplimiento para considerar la extinción contractual, sino únicamente aquel incumplimiento relevante o reiterado que afecte de manera grave a una obligación esencial, y por tanto, pueda poner en compromiso la continuidad natural del servicio y frustre la expectativa de la finalidad perseguida por la contraparte al suscribir el contrato⁷⁶.

Un incumplimiento sustancial del contrato de los servicios de computación en la nube por parte del proveedor puede consistir en no facilitar el acceso continuado a las capacidades, o que estas no se entreguen en las condiciones pactadas y dejen de tener utilidad para el cliente, impidiendo que pueda satisfacer las necesidades que le llevaron a contratar el servicio⁷⁷. El cliente, por su parte, podría

incumplimiento. Cada una de las partes puede suspender el cumplimiento o rescindir este Acuerdo si i) la otra parte incumple de forma sustancial el Acuerdo y no lo subsana antes de treinta días después de la recepción de la notificación por escrito, ii) la otra parte cesa sus operaciones empresariales o se ve sometida a procedimientos de insolvencia y dichos procedimientos no se desestiman antes de noventa días o iii) la otra parte incumple este Acuerdo de forma sustancial más de dos veces, sin perjuicio de la subsanación de dichos incumplimientos". Cláusula extractada de las condiciones generales del Software como Servicio (SaaS) *G-Suite* [en línea], <https://gsuite.google.com/intl/es/terms/2013/1/premier_terms.html>. [Fecha de consulta: 15 de febrero de 2017].

75 Art. 1124 del Código Civil: "La facultad de resolver las obligaciones se entiende implícita en las recíprocas, para el caso de que uno de los obligados no cumpliera lo que le incumbe. El perjudicado podrá escoger entre exigir el cumplimiento o la resolución de la obligación, con el resarcimiento de daños y abono de intereses en ambos casos. También podrá pedir la resolución, aun después de haber optado por el cumplimiento, cuando éste resultare imposible. El Tribunal decretará la resolución que se reclame, a no haber causas justificadas que le autoricen para señalar plazo. (...)".

76 El art. 1124 del Código Civil, pese a su inicial simplicidad, ha dado lugar a múltiple jurisprudencia, entre la cual destaca la Sentencia del Tribunal Supremo de 16 de abril de 1991. Esta sentencia afirma que la jurisprudencia "exige para la viabilidad de la acción resolutoria la prueba de los siguientes requisitos: a) la existencia d un vínculo contractual vigente entre quienes lo concertaron; b) la reciprocidad de las prestaciones estipuladas en el mismo, así como su exigibilidad; c) que el demandado haya incumplido de forma grave lo que le incumbía; d) que semejante resultado se haya producido como consecuencia de una conducta de este que de un modo indubitado, absoluto, definitivo e irreparable lo origine; y e) que quien ejercita la acción no haya incumplido las obligaciones que le concernían, salvo si ello ocurriera como consecuencia del incumplimiento anterior del otro, pues la conducta de este es lo que motiva el derecho a la resolución de su adversario y lo libera de su compromiso". Esta sentencia ha sido objeto de diversas puntualizaciones efectuadas por la doctrina, aunque por no centrar el objeto de este trabajo, no nos detendremos a analizarlas en detalle. Para ello, nos remitimos a DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. II. Las relaciones obligatorias*, 6ª Edición, Navarra, 2007, pág. 817 y ss.

77 Si el incumplimiento afecta a prestaciones accesorias, en cuanto que no afectan a la esencia del contrato, no supondrán una justa causa de resolución contractual. DIEZ-PICAZO, Luís,

CAPÍTULO SÉPTIMO

incumplir sustancialmente el contrato impagando las cuotas adeudadas o infringiendo las prohibiciones o restricciones establecidas a través de la política de uso adecuado del servicio (PUA).

La exigencia de un incumplimiento grave para poder resolver el contrato no implica que no se admita el incumplimiento parcial como incumplimiento resolutorio, siempre y cuando este incumplimiento parcial sea significativo y afecte a una obligación esencial. Todo ello se acepta porque el art. 1124 no distingue entre ejecución parcial o total, aunque la buena fe deberá moderar este derecho de resolución para evitar abusos⁷⁸.

Cuando el motivo del incumplimiento es una prestación defectuosa, el alcance del defecto debe igualmente ser ponderado. En este sentido, como se señala en sede de teoría general, únicamente se permitirá la resolución del contrato en aquellos casos en los que la tara impida la utilidad del servicio para el fin inicialmente previsto, o en aquellas ocasiones en las que el deudor se niegue a corregir la deficiencia, siempre que esta corrección no implique una excesiva dificultad o carga al deudor, y permita así que el servicio vuelva a ser útil.

Trasladando esta afirmación al ámbito de la computación en la nube, podemos deducir que, por ejemplo, cuando tengan lugar continuadas interrupciones o errores del servicio, u otras alteraciones que entorpezcan significativamente la agilidad exigida en el suministro, se permitirá rescindir el contrato, ya que de otro modo resultaría impracticable el acceso continuado a la capacidad informática contratada, y se produciría una merma considerable en la utilidad práctica del servicio suscrito. En el caso de que esos incumplimientos parciales no lleguen a ser lo suficientemente relevantes para extinguir la relación contractual, puede considerarse la operatividad de otros mecanismos de compensación, como por ejemplo los *service credits*⁷⁹.

Cuando el retraso sucede en el pago, generalmente se producirá, de forma

Fundamentos del Derecho Civil Patrimonial, Vol. II. Las relaciones obligatorias, 6ª Edición, Navarra, 2007, pág. 867.

78 DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. II. Las relaciones obligatorias*, 6ª Edición, Navarra, 2007, pág. 830.

79 Ver apartado "El cumplimiento defectuoso y la determinación de *service credits* como indemnización al cliente", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de computación en la nube".

CAPÍTULO SÉPTIMO

previa a la resolución contractual, un requerimiento por parte del proveedor. Si este requerimiento no es atendido, el impago es susceptible de considerarse incumplimiento sustancial y, según el procedimiento establecido en el contrato, puede dar lugar a la suspensión del servicio y a su posterior cancelación.

En cuanto al resarcimiento de los daños ocasionados por el incumplimiento, exigibles también en el caso en el que se proceda a la resolución del contrato por este motivo (art. 1124 del Código Civil), deberemos estar a la distribución de riesgos y responsabilidades entre las partes, especialmente si el acuerdo lo suscribe un pequeño empresario⁸⁰.

4.1.3.- La imposibilidad sobrevenida de continuar con la prestación del servicio

Cuando el servicio *cloud* no puede prestarse debido a una imposibilidad sobrevenida, absoluta y definitiva no imputable al deudor, se afirma por la doctrina que en este caso puede resolverse la obligación⁸¹. Sin embargo, todo lo anterior cambia cuando contractualmente se ha establecido una forma distinta de distribuir los riesgos entre ambas partes.

Los grandes proveedores suelen disponer de centros de datos redundantes entre los cuales se producen replicados de información, con lo cual se aseguran así la continuidad del servicio incluso en aquellos casos en los que un evento catastrófico, político o de otra índole que afecte a uno de los centros de datos les impida continuar con la prestación continuada del servicio. Aun así, son habituales las exenciones de responsabilidad en cuanto al suministro en caso de fuerza mayor que impida la prestación del servicio⁸².

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

81 DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. II. Las relaciones obligatorias*, 6ª Edición, Navarra, 2007, pág. 839.

82 Veamos como regula el proveedor *Acens* que acontezca una causa de fuerza mayor: "Ninguna de las partes será responsable del retraso en la ejecución de sus obligaciones ni de la no ejecución de las mismas (exceptuando el incumplimiento de pago a la otra parte) si este incumplimiento estuviese motivado por casos fortuitos o razones de fuerza mayor, de conformidad con lo establecido en el artículo 1.105 del Código Civil. Esta circunstancia se comunicará a la otra parte en el plazo más breve posible. Los plazos de entrega acordados se prolongarán en al menos el período de tiempo que haya durado la causa de fuerza mayor. Si la causa de fuerza mayor se prolonga más de tres (3) meses, cualquiera de las partes podrá resolver estas Condiciones de Contratación, sin perjuicio del cumplimiento de las obligaciones de pago debidas hasta la fecha previa. La causa fortuita o los eventos de fuerza mayor, así como la terminación de las Condiciones de

CAPÍTULO SÉPTIMO

Además de la fuerza mayor o el incumplimiento, las propias cláusulas contractuales pueden incluir otros motivos que fundamenten la resolución del contrato, como la falta de solvencia de una de las partes⁸³.

4.2.- Efectos de la extinción del contrato de computación en la nube

Entre las cuestiones que más preocupan al cliente de servicios de computación en la nube se encuentra el desconocimiento del destino de sus datos una vez que se extinga la relación con el proveedor⁸⁴. Especialmente, dos son las cuestiones que sobrevuelan tal incertidumbre: la primera, si se le permitirá recuperar esos datos o aplicaciones para usarlos con otro proveedor o instalarlos de nuevo en sus propios sistemas, comúnmente conocida como portabilidad. La segunda, si el proveedor retendrá esos contenidos para sí o para terceros, o si serán borrados totalmente de sus sistemas, convirtiéndolos en irrecuperables. Ambas cuestiones (portabilidad y borrado) integran lo que se entiende como "reversibilidad del servicio de computación en la nube", cuestión de gran importancia práctica en este tipo de servicios⁸⁵.

Contratación fundamentada en las anteriores, no exonerará al Cliente del cumplimiento de las obligaciones de pago pendientes hasta la fecha de interrupción de los Servicios". Condiciones generales de Acens [en línea]. Disponibles en: <http://www.acens.com/file_download/condiciones_generales_de_contratacion_electronica_acens.pdf>. [Fecha de consulta: 15 de febrero de 2017].

- 83 Las condiciones generales para contratar servicios de Acens establecen otras causas de terminación del contrato: "Sin perjuicio de todo lo anterior, las partes podrán terminar la relación en cualquier momento, en el supuesto que la otra parte: (a) incumpla grave o reiteradamente las obligaciones asumidas en el presente documento; (b) entre en liquidación voluntaria u obligatoria (excluida toda reorganización o fusión) o en proceso de suspensión de pagos o quiebra; (c) entre o decida entrar en algún tipo de negocio jurídico o procedimiento por el que todos o una parte importante de sus activos pasen a beneficio de sus acreedores en general, o de algunos en particular; (d) un tribunal acuerde su liquidación y/o disolución, y/o se nombre un administrador judicial u otro cargo similar en relación a la totalidad o alguna parte de sus activos o patrimonio y (e) en caso de darse cualquiera de las causas previstas en las leyes". Cláusula extractada de las condiciones generales de servicios Acens [en línea], Disponibles en: <https://www.acens.com/file_download/condiciones_generales_de_contratacion_electronica_acens.pdf>. [Fecha de consulta: 15 de febrero de 2017].
- 84 KUAN HON, W; MILLARD, C, WALDEN, I, "Negotiated Contracts for Cloud Services", *Cloud Computing Law*, (coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 73.
- 85 El estándar ISO/IEC 17788:2014 definió la reversibilidad como el proceso para clientes de servicios *cloud* que les permite recuperar sus datos y aplicaciones como clientes, y el proceso que

CAPÍTULO SÉPTIMO

Por último, estudiaremos como se lleva a cabo el borrado de archivos en sistemas de computación en la nube y las consecuencias jurídicamente relevantes que se desprenden para las partes.

5.-LA RECUPERACIÓN DE LOS CONTENIDOS ALOJADOS EN LA NUBE POR EL CLIENTE Y SU PORTABILIDAD A OTRO PROVEEDOR *CLOUD*

Como se ha mencionado, el momento de la prestación del servicio de computación en la nube en el cual trasciende la relevancia de la recuperación y la portabilidad de los contenidos alojados remotamente tiene lugar cuando el nexo contractual llega a su fin⁸⁶. En ese instante, el cliente es consciente de la necesidad de recuperar del sistema del proveedor los contenidos migrados. Una recuperación que pretende ser definitiva e irreversible, efectuada con la finalidad de transferir esa información digital a la nube de otro proveedor o de incorporarla a sus sistemas propios, y que alcance todo el material que el cliente haya podido alojar en la nube: datos personales, datos de carácter no personal, metadatos, aplicaciones, etc.⁸⁷ No obstante lo anterior, consideramos que el derecho a la portabilidad de los datos migrados debería poder ejercitarse no solo una vez se produzca la extinción del contrato, sino en cualquier momento de la prestación en el cual el suscriptor decida,

permite al proveedor borrar todos los datos de sus clientes así como los datos derivados de la interacción del cliente con el servicio, después del plazo acordado. (Traducción propia). Estándar Internacional ISO/IEC 17788:2014. *Information Technology - Cloud Computing-Overview and Vocabulary* [en línea]. Disponible en: <http://www.iso.org/iso/catalogue_detail?csnumber=60544>. [Fecha de consulta: 15 de febrero de 2017].

86 Para un estudio más amplio, nos remitimos a ROSSELLÓ RUBERT, Francisca M^a, "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.

87 Dicho de otro modo, el orden natural de acontecimientos una vez extinguido el contrato es: en primer lugar, el acceso a los contenidos almacenados; en segundo lugar, su posibilidad de recuperación o descarga por el cliente, si este lo desea, ejercitable durante un plazo de tiempo determinado por el proveedor. Cuando esa recuperación se produce en un formato útil que no implique volver a introducir esos contenidos mecánicamente, se puede afirmar que existe portabilidad. Si no, únicamente existe una recuperación de datos no portables. Y, en tercer lugar, el borrado de los datos del cliente de los sistemas del proveedor, cuya cuenta ya ha sido inhabilitada de forma definitiva.

CAPÍTULO SÉPTIMO

por los motivos que fuesen, recuperar los contenidos migrados a los sistemas del proveedor a la vez que la prestación continúa teniendo lugar.

Respecto de la portabilidad, entendida como la capacidad de transferir fácilmente contenidos entre diferentes sistemas, hemos mencionado que puede afectar a diferentes contenidos, como son los datos y las aplicaciones. La portabilidad de los datos ha sido definida técnicamente como "la capacidad de transferir de manera sencilla los datos de un sistema o otro sin necesidad de volver a introducirlos"⁸⁸. Pero, además, puede ser esencial en suministros de infraestructura (IaaS) o plataforma (PaaS) "la capacidad del sistema para migrar una aplicación de un servicio *cloud* a otro servicio *cloud* de un proveedor distinto", es decir, la portabilidad de las aplicaciones.

Seguidamente, analizaremos las diferencias técnicas que alcanzan los conceptos portabilidad de datos y portabilidad de aplicaciones; y el vínculo existente entre la portabilidad y el formato de los contenidos en los entornos de la nube. Posteriormente, dejaremos atrás la distinción entre ambos conceptos, englobándolos bajo el concepto de portabilidad de los contenidos del cliente, para analizar su configuración jurídica.

En cuanto a esta configuración jurídica, queremos adelantar que la portabilidad puede ser considerada desde distintos ángulos, dependiendo de la perspectiva del legislador, del proveedor de servicios *cloud* y del cliente que los suscribe. Consecuencia de ello es un marco jurídico insuficiente, una inseguridad jurídica del cliente respecto a la devolución de sus datos en un formato útil, y el beneficio que supone este panorama para los intereses de los proveedores de servicios de computación en la nube. Todo ello será objeto del apartado que nos ocupa.

88 El estándar ISO/IEC 17788:2014 definió la portabilidad de datos como "*ability to easily transfer data from one system to another without being required to re-enter data*" (traducción propia), y concreta el mismo documento que la esencia de la portabilidad es la facilidad del traslado, y aunque los formatos de emisión y recepción de información no coincidan, la transformación debe poder lograrse a través de herramientas fácilmente accesibles y manejables. con lo cual la impresión de la información y su posterior tecleado para volver a introducirlo en el sistema, como puntualiza el informe, no tiene la consideración de "fácil o sencillo". Por otra parte, la portabilidad de las aplicaciones se define en el mismo estándar con estos términos: "*ability to migrate an application from one cloud service to another cloud service*" (traducción propia). Estándar Internacional ISO/IEC 17788:2014. *Information Technology - Cloud Computing-Overview and Vocabulary* [en línea]. Disponible en: <http://www.iso.org/iso/catalogue_detail?csnumber=60544>. [Fecha de consulta: 4 de abril de 2017].

CAPÍTULO SÉPTIMO

5.1.-La portabilidad de los datos y la portabilidad de las aplicaciones

Dentro de los contenidos que el cliente migra a la nube del proveedor, es posible diferenciar entre los datos digitales y las aplicaciones informáticas. Por ello distinguiremos, en primer lugar, entre la portabilidad de los datos y la portabilidad de las aplicaciones.

Aunque se utiliza de forma generalizada el término "portabilidad de datos" para hacer referencia a la recuperación del conjunto de información migrada por el cliente, lo cierto es que existen diferencias técnicas entre la portabilidad de programas informáticos (más concretamente, aplicaciones) y aquella que transfiere otros datos o archivos informáticos (documentos de texto, imágenes, etc.).

En cuanto a la portabilidad de los datos, la utilidad de la portabilidad es que puedan trasladarse al nuevo entorno de manera sencilla, sin necesidad de volver a introducir manualmente o teclear toda la información de nuevo.

La portabilidad de las aplicaciones informáticas que el cliente haya podido migrar y ejecutar en infraestructuras (IaaS) o plataformas (PaaS) proporcionadas por el proveedor *cloud*, además, presenta sus propios problemas. Estas aplicaciones se integran en la API (*Application Programming Interface*) del proveedor, pero puede resultar complicado migrar aplicaciones para que se puedan ejecutar en equipos que carezcan de esta misma API, ya que los proveedores no siempre permiten el uso de sus API fuera de su entorno *cloud*⁸⁹. Por ello, ante la falta de protocolos estándar establecidos⁹⁰, es recomendable que el pequeño empresario que pretenda desarrollar

89 Las API son conjuntos de software que permiten la integración de aplicaciones, codificadas en distintos lenguajes informáticos y ejecutables en diferentes plataformas, permitiendo la interacción entre estas y otras aplicaciones, sistemas operativos, dispositivos y entornos *cloud* (es decir, su interoperabilidad), y facilitan la portabilidad de contenidos entre diferentes proveedores de la nube. REED, Cris; CUNNINGHAM, Alan, "Ownership of Information in Clouds", *Cloud Computing Law*, (coord. Christopher Millard), Oxford, 2013, pág. 161.

90 La Comisión Europea, en el marco de la *Cloud Computing Strategy*, impulsó la coordinación entre los diferentes operadores del sector de computación en la nube, y publicó un informe con los principales aspectos relacionados con la adopción de estándares tecnológicos de entornos *cloud*. En este documento, que lleva por título "*Cloud Standards Coordination-Final Report*", se recogen el estado de la técnica y de los servicios ofrecidos por proveedores desde una perspectiva global, una lista con más de 20 organizaciones relevantes en materia de adopción de estándares técnicos para entornos de nube, así como una recopilación de documentos relacionados. De las

CAPÍTULO SÉPTIMO

o ejecutar aplicaciones en la nube sea previsor, y obtenga la máxima información posible, antes de contratar los servicios, sobre los sistemas de integración que permitan la portabilidad de las aplicaciones, que se interese por formatos libres o lo suficientemente extendidos para permitir portarlos a otros proveedores⁹¹; y que calcule el posible coste de salida del servicio⁹².

De lo anterior se desprende que la portabilidad irá vinculada al formato de retorno de los contenidos. De este modo, cuando estos contenidos migrados por el cliente (sean aplicaciones software u otro tipo de datos) puedan transportarse con facilidad a otro sistema *cloud*, sin tener que volver a teclearlos, reescribirlos o reprogramarlos, podremos hablar de portabilidad de contenidos.

Es importante remarcar, en relación al formato de devolución de los contenidos, que es habitual que no se detallan contractualmente los detalles técnicos de la recuperación de los contenidos del cliente, entre los que se encuentra la definición del formato en el cual pueden recuperarse, o si se trata de la recuperación

conclusiones del informe se extrae que el ámbito de estándares *cloud* es amplio, pero no caótico, sino abarcable a medio plazo; que son especialmente relevantes los estándares relacionados con la interoperabilidad, la seguridad y los niveles de servicio, y que la diversidad de legislación multinacional involucrada puede implicar barreras en cuanto a la adopción de estándares. El informe final está disponible en el sitio web de la Comisión Europea: <<https://ec.europa.eu/digital-single-market/en/news/cloud-standards-coordination-final-report>>. [Fecha de consulta: 4 de abril de 2017].

91 HON, W. Kuan; MILLARD, C, "Control, Security, and Risk in the Cloud", *Cloud Computing Law*, (coord. Christopher Millard), Oxford, 2013, pág. 26.

92 El grupo de expertos de la *Cloud Computing Strategy* consideró, en su *Discussion Paper* de 29 de enero de 2014, que los entornos de computación en la nube integran diferentes sistemas operativos y bases de datos. Cada entorno contiene diferentes concepciones técnicas del servicio de computación en la nube (máquinas virtuales, procesos, protocolos de seguridad, modelos de almacenamiento, redes, API, softwares licenciados, etc.). Así, los principales problemas de la portabilidad son, según los mismos expertos, esta falta de homogeneidad en cuanto a la concepción técnica, la variedad de equipos y sistemas *cloud* del mercado, las diferentes exigencias y circunstancias de los proveedores (uso de posición dominante del mercado, etc.), la existencia de cadenas de proveedores que dificulta la recolección de datos, y la falta de homogeneidad en las condiciones contractuales predispuestas por los proveedores, entre otras causas. En el mismo sentido, según comentaron algunos expertos del sector empresarial *cloud*, la definición y adopción de estándares de interoperabilidad resulta compleja, puesto que la innovación y el cambio en la industria son más veloces que cualquier proceso de estandarización. Estas declaraciones tuvieron lugar durante el evento *Cloud Expo Europe London* de 2014. Información disponible en: <<https://www.nexica.com/es/blog/interoperabilidad-en-la-nube>>. El informe de los expertos de la *Cloud Computing Strategy* está disponible también en línea: <http://ec.europa.eu/justice/contract/files/expert_groups/discussion_paper_topic_4_switching_en.pdf>. [Fecha de consulta: 4 de abril de 2017].

CAPÍTULO SÉPTIMO

de una copia de los datos migrados o de la transferencia de todos los contenidos del cliente que el proveedor almacena. La delimitación de un formato al inicio del contrato puede ser difícil, puesto que estos contratos se suscriben con intención de ser duraderos, y la tecnología informática avanza con rapidez, con lo cual un formato inicialmente útil puede, con el tiempo, quedar desfasado o no adecuarse a las necesidades que el cliente hubiera previsto en un primer momento.

En este caso, cabría la opción de que el proveedor, en interés del conocimiento de este formato por el cliente, modificase las condiciones contractuales cada vez que considerase adecuado adoptar un formato de recuperación de datos diferente al inicialmente previsto. De todos modos, la información relativa al formato de recuperación generalmente se produce a petición del cliente, ya sea de manera previa a la suscripción del contrato (lo cual es más que recomendable), ya sea justo antes de proceder a la recuperación definitiva de los contenidos migrados.

La elección del formato "utilizable" se concibe de manera diferente dependiendo del proveedor. Las Directrices adoptadas por la Unión Europea dentro de la *Cloud Computing Strategy* en materia de Acuerdos de Nivel de Servicio definen los diferentes parámetros de referencia, en relación a la portabilidad de los contenidos, los cuales se recomienda introducir en los contratos; parámetros que determinará cada proveedor en atención al tipo de servicio que suministre⁹³. Estos parámetros serán, principalmente, la portabilidad de formato (que especifica el formato electrónico que permitirá al cliente *cloud* transferir los datos) y la portabilidad de interfaz (que detalla los mecanismos que pueden usarse para transferir datos y aplicaciones del cliente, como especificaciones de protocolos de transporte y detalles sobre las API o sobre cualquier otro mecanismo de soporte de datos en la nube).

Las previsiones contractuales en relación a la portabilidad son útiles, aunque heterogéneas: en ellas encontramos proveedores que garantizan la portabilidad de los contenidos y otros proveedores que no la garantizan (por ejemplo, que mencionan realizar "esfuerzos comercialmente razonables"), e incluso contratos que no hacen referencia a la portabilidad. Aunque en ocasiones el cliente pueda reclamar

93 *Cloud Service Level Agreement Standardisation Guidelines* [en línea]. Disponible en: <<https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>>. [Fecha de consulta: 4 de abril de 2017]

CAPÍTULO SÉPTIMO

compensaciones ante pérdidas de datos o retenciones injustificadas, puede encontrarse sin posibilidad de recuperar sus contenidos⁹⁴. Veamos con más detalle algunos aspectos sobre la recuperación de los contenidos migrados por parte del cliente *cloud* una vez terminada la relación contractual.

5.2.- La expectativa de recuperación de los contenidos

Durante la prestación ordinaria del servicio, y con el fin de aprovechar las capacidades y/o funcionalidades contratadas, el cliente generalmente exporta o migra contenidos (datos y aplicaciones) de sus propios sistemas al entorno de nube que el proveedor pone a su disposición. Por contrapartida, de las obligaciones del proveedor inherentes a la naturaleza propia del servicio se desprende la custodia de esos datos, garantizando su seguridad (es decir, su integridad, confidencialidad y disponibilidad) y, una vez finalizado el servicio, procederá a la devolución de los datos migrados del cliente⁹⁵.

Así, la recuperación de los contenidos genera una expectativa legítima en el cliente, quien ha confiado en el proveedor para almacenar los contenidos digitales en sus sistemas, con la esperanza de que serán conservados de modo seguro, íntegro y confidencial, que estarán disponibles mientras dure la prestación del servicio, y que podrá rescatarlos una vez el servicio llegue a su fin⁹⁶.

Los expertos del grupo de trabajo sobre contratación de la *Cloud Computing Strategy* consideran las retenciones injustificadas de contenidos del cliente una vez extinguido el contrato de alojamiento remoto como un ejemplo de cláusula abusiva, por carecer de proporcionalidad entre derechos y obligaciones de las partes⁹⁷. Se

94 HON, W. Kuan; MILLARD, C, *Control, Security and...*, *op. cit.*, pág. 26.

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

96 En el mismo sentido se concibió en la Propuesta de Código Mercantil: el permitir la recuperación de los datos alojados se integra como una de las las obligaciones esenciales del prestador del alojamiento de datos. "Artículo 532-13. Obligaciones del prestador del servicio de alojamiento de datos. 1. Será obligación del prestador de alojamiento de datos poner a disposición del cliente la capacidad de almacenamiento pactada en un sistema de información bajo su control, así 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".

97 Síntesis de 5 y 6 de marzo de 2014, del Grupo de Expertos en contratos de computación en la nube, de la *European Cloud Computing Strategy* [en línea]. Disponible en:

CAPÍTULO SÉPTIMO

plantea este grupo si debería hacerse una distinción al respecto entre los servicios sujetos a contraprestación económica y los que no lo están, y si pueden existir elementos específicos de los servicios de computación en la nube que motiven esta falta de equilibrio.

A continuación, trataremos esta expectativa de recuperación de los contenidos de cualquier cliente de servicios de computación en la nube, tanto desde el punto de vista de ambas partes contractuales como desde el punto de vista del legislador.

5.2.1.-La retención de contenidos por parte del proveedor y su relación con la contraprestación económica del servicio *cloud*

Respecto de si es oportuno que el proveedor retenga contenidos del cliente en aquellos contratos "gratuitos", como hemos manifestado en anteriores ocasiones, consideramos que la falta de contraprestación económica puede ejercer un papel moderador en la distribución de riesgos entre las partes⁹⁸. Sin embargo, en el caso del retorno de contenidos es irrelevante que el servicio se preste sin retribución pecuniaria, puesto que se ha generado una expectativa en el cliente que se fundamenta en las características propias de la naturaleza de los servicios *cloud* que suponen el alojamiento remoto, y se desprende de ellas que, si el proveedor tiene obligación de custodiar sus contenidos, también se debe permitir al cliente recuperarlos. Por tanto, formará parte del deber de diligencia del proveedor garantizar, por una parte, disponibilidad, integridad y confidencialidad de esos contenidos y, por otra parte, poner a disposición del cliente esos datos para que pueda procederse a su recuperación cuando el contrato se extinga⁹⁹.

Sin embargo, en la práctica, el coste de la recuperación de los datos no siempre recae sobre la posición del prestador de servicios, ya que, a falta de normativa específica que regule estas cuestiones para el cliente pequeño empresario, dependerá de la política comercial del prestador de servicios si los soporta o si los

<http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 4 de abril de 2017].

98 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.

99 Ver apartado "Obligaciones del proveedor", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

CAPÍTULO SÉPTIMO

traslada al cliente¹⁰⁰. De hecho, el grupo de expertos de la *Cloud Computing Strategy* reconoce que el cliente debería acostumbrarse a pagar por la devolución de los datos, aunque no realiza distinción alguna entre contratos onerosos y contratos sin contraprestación económica¹⁰¹.

Nosotros consideramos que la puesta a disposición de los contenidos para que el cliente pueda rescatarlos debe considerarse parte integrante de la naturaleza de aquellos contratos de computación en la nube que impliquen migraciones, independientemente de que esos contenidos comprendan datos de carácter personal, ya que, en base a esta naturaleza de alojamiento remoto, el cliente ha generado expectativas legítimas e intereses merecedores de protección.

Estos intereses pueden ser especialmente sensibles en aquellos casos en los que el cliente sea un pequeño empresario o profesional cuya actividad económica pueda depender, en mayor o menor medida, de la información confiada al proveedor. Por ello, creemos que, aunque el proveedor es libre de disponer el negocio jurídico como gratuito u oneroso por los servicios que oferta, no cabe configurar el retorno de los datos como una prestación accesorio, sino que, como hemos manifestado, consideramos esta obligación como inherente al propio servicio *cloud* de almacenamiento remoto de información digital.

5.2.2.- La retención de contenidos por parte del proveedor y su relación con la causa de extinción del contrato

Hemos comentado que los expertos del grupo de trabajo sobre contratación de la *Cloud Computing Strategy* han sometido a debate si pueden existir elementos específicos de los servicios de computación en la nube que motiven la retención de

100 Si se aprueba la Propuesta de Directiva de suministro de contenidos digitales, el cliente de servicios de suministros digitales que sea consumidor y resuelva el contrato, tendrá derecho a recuperar esos contenidos no solo sin costes, sino también sin impedimentos, en un plazo razonable y en un formato de uso habitual, según sus artículos 13 y 16. A lo largo de este apartado nos detendremos más profundamente en esta cuestión. Sin embargo, esto no regirá, en principio, en beneficio de aquellos clientes que no entren en la categoría legal de consumidor, como los pequeños empresarios.

101 El grupo de expertos en contratos de computación en la nube realiza esta afirmación en la síntesis de sus reuniones de 11 y 12 de diciembre de 2014 [en línea]. Disponibles en: <http://ec.europa.eu/justice/contract/files/7th_expert_group_synthesis_final.pdf>. [Fecha de consulta: 4 de abril de 2017]

CAPÍTULO SÉPTIMO

los contenidos del cliente. A continuación, expondremos la situación actual y las implicaciones jurídicas de este tema¹⁰².

Algunos proveedores distinguen entre las diferentes causas de terminación del contrato en cuanto a la determinación de costes para recuperar los datos. Así, el proveedor en ocasiones opta por descargar sobre el cliente los costes de la recuperación de los contenidos, tal y como hemos apuntado en el apartado anterior. Esta concepción de la recuperación de contenidos como un servicio añadido puede venir motivada por una decisión comercial que afecte por igual a todos los suscriptores, o ir vinculada al motivo de terminación del contrato, trasladando los costes sobre aquel cliente que decida terminar el contrato por mera conveniencia, que incumpla el pacto de preaviso de la intención de no prorrogar el contrato, que se encuentre en situación de morosidad, etc.

Si bien en los párrafos siguientes de este mismo apartado plantearemos los diferentes efectos legales de esa retención en cuanto afecte o no a datos de carácter personal, es interesante preguntarse si el derecho a recuperar los datos opera por igual en todos los motivos de terminación del contrato. Por ejemplo, pueden presentarse dudas acerca de si es o no razonable que el proveedor prive al cliente de acceder a sus datos o recuperarlos cuando la causa de terminación sea el incumplimiento de la obligación de pago del cliente o un abuso del servicio que atente gravemente contra las prohibiciones contempladas en la política de uso adecuado (PUA).

En nuestra opinión, aunque el proveedor haya suspendido la prestación al cliente y le haya denegado el acceso a sus contenidos de manera temporal debido a ese incumplimiento, la falta de pago no exime al proveedor de la obligación de permitir recuperar al cliente sus contenidos si finalmente se extingue la relación jurídica, sin perjuicio de que posteriormente reclame al cliente los importes devengados a través de los cauces legales habituales y decida rescindir el contrato (art. 1124 del Código Civil¹⁰³). La expectativa del cliente de recuperar los datos trae

102 Síntesis de 5 y 6 de marzo de 2014, del Grupo de Expertos en contratos de computación en la nube, de la *European Cloud Computing Strategy* [en línea]. Disponible en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 4 de abril de 2017].

103 Art. 1124 del Código Civil: "La facultad de resolver las obligaciones se entiende implícita en las recíprocas, para el caso de que uno de los obligados no cumpliere lo que le incumbe. El perjudicado podrá

CAPÍTULO SÉPTIMO

causa en el propio objeto del contrato, y por tanto, aunque *a posteriori* haya incumplido su obligación de pago por los motivos que fueren, ello no puede afectar a la obligación del proveedor de posibilitar la recuperación de los contenidos que el cliente le confió desde los inicios del servicio, ni habilita a aquel a establecer como penalización por el incumplimiento la retención de tales contenidos.

Como veremos más adelante, parece que la Propuesta de Directiva de suministro de contenidos digitales ha tenido en cuenta la expectativa legítima de recuperación de contenidos que se genera en el cliente de servicios de suministros de contenidos digitales, y por ello dota al consumidor de un derecho a recuperar los datos generados por el uso del servicio y migrados, sin costes ni impedimentos, en un plazo razonable y en un formato de uso habitual. Sin embargo, el pequeño empresario o profesional carece, de momento, de esta facultad legal.

Por otra parte, si el servicio de portabilidad se fija desde el primer momento como un servicio accesorio sujeto a un pago añadido, opinamos que el proveedor deberá informar de manera previa y adecuada al cliente, ya que, en caso contrario, puede ser considerado una práctica desleal por engañosa, en cuanto se haya intentado ocultar la exigencia del pago por un servicio que inicialmente podría entenderse como obligación principal de la prestación, de acuerdo con la naturaleza del propio contrato *cloud* (arts. 5 y 7 de la Ley de Competencia Desleal, y art. 20 de la Ley General para la Defensa de Consumidores y Usuarios)¹⁰⁴ y contrario al

escoger entre exigir el cumplimiento o la resolución de la obligación, con el resarcimiento de daños y abono de intereses en ambos casos. También podrá pedir la resolución, aun después de haber optado por el cumplimiento, cuando éste resultare imposible. (...)"

104 Artículo 5 de la Ley de Competencia Desleal: "Se considera desleal por engañosa cualquier conducta que contenga información falsa o información que, aun siendo veraz, por su contenido o presentación induzca o pueda inducir a error a los destinatarios, siendo susceptible de alterar su comportamiento económico, siempre que incida sobre alguno de los siguientes aspectos: (...) a) El precio o su modo de fijación, o la existencia de una ventaja específica con respecto al precio.(...) f) La necesidad de un servicio o de una pieza, sustitución o reparación". Artículo 7 de la Ley 3/1991 de 10 de enero de Competencia Desleal: "Omisiones engañosas. 1. Se considera desleal la omisión u ocultación de la información necesaria para que el destinatario adopte o pueda adoptar una decisión relativa a su comportamiento económico con el debido conocimiento de causa. (...)". Art. 20 Ley General para la Defensa de los Consumidores y Usuarios: "Las prácticas comerciales que, de un modo adecuado al medio de comunicación utilizado, incluyan información sobre las características del bien o servicio y su precio, posibilitando que el consumidor o usuario tome una decisión sobre la contratación, deberán contener, si no se desprende ya claramente del contexto, al menos la siguiente información: Las características esenciales del bien o servicio de una forma adecuada a su naturaleza y al medio de comunicación utilizado. El precio final completo, incluidos los impuestos, desglosando, en su caso, el importe de los incrementos o descuentos que sean de aplicación a la oferta y los gastos adicionales que se repercutan al consumidor o usuario. En el resto de los casos en que, debido a la naturaleza del bien o servicio, no pueda fijarse con exactitud el precio en la

CAPÍTULO SÉPTIMO

comportamiento honesto que se espera del empresario profesional que puede provocar distorsiones en el comportamiento del consumidor (art. 4.1 Ley de Competencia Desleal)¹⁰⁵.

Cuando el incumplimiento del cliente está relacionado con la infracción de la política de uso adecuado (PUA) con la cual se había comprometido, quizá podría razonarse alguna excepción al deber de restitución, cuando con esta se produzcan perjuicios al proveedor, al resto de usuarios del servicio *cloud* o a terceros, o se entorpezca una investigación de autoridades competentes¹⁰⁶. De todos modos, consideramos que, puesto que el proveedor se posiciona como único juzgador (al menos, *a priori*¹⁰⁷) sobre la continuidad de la prestación ante una presunta violación de la política de uso adecuado, para que este incumplimiento impida devolver al cliente sus contenidos debe tratarse de una inobservancia suficientemente grave, o que con la restitución puedan perjudicarse otros intereses merecedores de ser igualmente protegidos, como por ejemplo, derechos de propiedad intelectual de terceros, la utilización segura del servicio por parte de otros usuarios, etc.

Hasta el momento hemos expuesto nuestra posición en relación a la puesta a disposición del cliente de los contenidos migrados en un formato manejable para que este pueda recuperarlos como una obligación del contrato de computación en la

oferta comercial, deberá informarse sobre la base de cálculo que permita al consumidor o usuario comprobar el precio. Igualmente, cuando los gastos adicionales que se repercutan al consumidor o usuario no puedan ser calculados de antemano por razones objetivas, debe informarse del hecho de que existen dichos gastos adicionales y, si se conoce, su importe estimado. El incumplimiento de lo dispuesto en el apartado anterior será considerado práctica desleal por engañosa en iguales términos a los que establece el artículo 7 de la Ley 3/1991, de 10 de enero, de Competencia Desleal".

105 Artículo 4.1 de la Ley de Competencia Desleal: "Se reputa desleal todo comportamiento que resulte objetivamente contrario a las exigencias de la buena fe. En las relaciones con consumidores y usuarios se entenderá contrario a las exigencias de la buena fe el comportamiento de un empresario o profesional contrario a la diligencia profesional, entendida ésta como el nivel de competencia y cuidados especiales que cabe esperar de un empresario conforme a las prácticas honestas del mercado, que distorsione o pueda distorsionar de manera significativa el comportamiento económico del consumidor medio o del miembro medio del grupo destinatario de la práctica, si se trata de una práctica comercial dirigida a un grupo concreto de consumidores. A los efectos de esta ley se entiende por comportamiento económico del consumidor o usuario toda decisión por la que éste opta por actuar o por abstenerse de hacerlo en relación con: (...) c) El pago del precio, total o parcial, o cualquier otra forma de pago.(...) e) El ejercicio de los derechos contractuales en relación con los bienes y servicios.

106 Pensamos en utilizations ilícitas del servicio, en las cuales los datos almacenados puedan constituirse como pruebas de una infracción de legislación, por ejemplo, en materia penal, tributaria, de patentes, etc.

107 Y sin perjuicio de posteriores valoraciones por las autoridades judiciales o arbitrales competentes sobre la pertinencia de la retención de los datos del cliente.

CAPÍTULO SÉPTIMO

nube que implique el alojamiento de datos. Sin embargo, nuestra posición sobre la portabilidad de la generalidad de contenidos migrados debe enlazarse con el derecho a la portabilidad que reconoce recientemente la nueva regulación europea en materia de privacidad a los titulares de datos de carácter personal¹⁰⁸. Para su estudio detallado, nos remitimos al capítulo dedicado a la protección de datos de este mismo trabajo.

5.2.3.- El derecho a la recuperación de los datos y a la portabilidad

Correlacionado con el deber de custodia del proveedor *cloud* en relación a los datos ajenos depositados en sus sistemas por razón de los contratos de servicios suscritos por sus clientes, debe entenderse el compromiso de devolver aquello depositado, que no le pertenece y no puede utilizar sin consentimiento, una vez finalizada la relación contractual¹⁰⁹. En caso contrario, parece evidente que se frustraría la causa propia del contrato *cloud* que implique un alojamiento remoto de datos del cliente, puesto que no tendría sentido contratar este tipo de servicios si los datos alojados únicamente pueden utilizarse dentro del equipo del proveedor, y no pueden ser recuperados por su titular en su totalidad y en un formato manejable que permita tratarlos o transmitirlos en entornos externos o de otro proveedor. Sin embargo, tras observar en la práctica del sector la redacción de las cláusulas relativas a los efectos de la terminación del contrato, parece que no existe unanimidad sobre si el proveedor asume la obligación de devolver esos datos en un formato útil.

108 Hasta la aparición del nuevo Reglamento General de Protección de Datos, el concepto de portabilidad únicamente aparecía recogido en la normativa española en relación a la conservación del número de teléfono cuando se produce un cambio de compañía por parte del titular de la línea, con el fin de no desincentivar al usuario que desee cambiar de proveedor de telefonía. Actualmente, este derecho se contempla en el artículo 21 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

109 En una aplicación analógica del contrato de depósito, el art. 1767 impide al depositario hacer uso de aquello depositado sin consentimiento expreso: "El depositario no puede servirse de la cosa depositada sin permiso expreso del depositante. En caso contrario, responderá de los daños y perjuicios". Afirma MARTIN SANTIESTEBAN que "el uso indebido de la cosa depositada constituye un incumplimiento de la obligación de custodiar, incompatible con la propia naturaleza del contrato [de depósito], ya que la cosa es depositada para satisfacer el interés del depositante en la custodia (y en su caso el del depositario en la remuneración), no el del depositario en el uso como es el caso del comodato". Queremos matizar esta afirmación en cuanto se aplique a contratos *cloud* sin contraprestación económica, en los cuales el proveedor únicamente podrá utilizar aquellos contenidos cedidos cuando el cliente haya consentido en ese uso a través de una cláusula contractual. MARTÍN SANTIESTEBAN, Sonia; *El depósito y la responsabilidad del depositario*, 1ª Edición, Navarra, 2002, pág.146.

CAPÍTULO SÉPTIMO

Contrariamente a lo que es de esperar, de la redacción de ciertas cláusulas se deduce que el proveedor, en algunas ocasiones, no asume como esencial la obligación de retornar los contenidos que el cliente alojó en sus sistemas, y se reserva el derecho a retenerlos o a devolverlos únicamente cuando se abone un precio añadido¹¹⁰.

Al ser el contrato de computación en la nube un contrato atípico, hemos señalado en capítulos anteriores varias similitudes con contratos ya existentes, siendo uno de ellos el contrato de depósito, en cuanto a la obligación del proveedor de guardar y restituir la cosa (en este caso, los contenidos digitales) confiada¹¹¹. Aplicando analógicamente la regulación del Código Civil en cuanto a la obligación de restitución del depósito, el proveedor de computación en la nube debería devolver los contenidos digitales cuando así se lo solicite al cliente, puesto que el contrato de computación en la nube implica la custodia de estos datos¹¹², y opinamos que la transmisión que tiene lugar durante la prestación ordinaria del contrato *cloud* no habilita al proveedor a retenerlos. Igualmente, creemos que, cuando el cliente lo solicite, deberá retornar aquellos contenidos cuyo uso expresamente haya cedido el cliente al proveedor de forma legítima, aunque ello no impida que el proveedor pueda quedarse con una copia de esos contenidos para ejercer los derechos que el cliente le haya transferido¹¹³.

110 "(...) Usted acepta que si se suspende o se da por terminado su acceso a los servicios, ya no podrá acceder al contenido almacenado mediante los servicios. A la terminación por parte de [el proveedor] de su acceso a los Servicios o su uso de los mismos, por razones distintas a motivo justificado, o por indicación de usted, puede solicitar el acceso a su contenido, que le facilitaremos por un importe adicional. Usted deberá realizar esa solicitud en los cinco (5) días siguientes a la terminación. De lo contrario, el contenido que usted haya almacenado mediante los servicios no se podrá recuperar, y no tendremos ninguna obligación de mantener los datos almacenados en su cuenta. (...)". Condiciones de uso del software como servicio (SaaS) de almacenamiento remoto de datos *Box* [en línea]. Disponible en: <<https://www.box.com/legal/termservice/ES/>>. [Fecha de consulta: 5 de abril de 2017].

111 Aplicando analógicamente el contrato de depósito, podemos afirmar la existencia de esta obligación en relación a los contenidos custodiados por el proveedor, de acuerdo con el art. 1770 del Código Civil: "La cosa depositada será devuelta con todos sus productos y accesiones". Además, afirma MARTÍN SANTISTEBAN que "El deber de restituir la cosa depositada ha de servir para integrar el contenido de la obligación de guarda y custodia", que " obligaciones de custodiar y restituir están interrelacionadas desde el punto de vista de la configuración causal del contrato", y que "ambas obligaciones son principales y autónomas". MARTÍN SANTISTEBAN, Sonia; *El depósito y la responsabilidad...*, op. cit., pág. 255-256. Ver capítulo "Objeto, naturaleza jurídica y características del contrato de servicios de computación en la nube".

112 Los datos migrados no pertenecen al proveedor, excepto que el cliente haya pactado lo contrario. Ver capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

113 De aquí, la importancia para el cliente de leer detenidamente las condiciones generales, para que no enmascaren cesiones de uso de datos que son propiedad del cliente. Ver capítulo "Aspectos

CAPÍTULO SÉPTIMO

En cuanto a los *metadatos*¹¹⁴, puede existir existe una titularidad compartida sobre ellos, puesto que son datos creados por los sistemas del proveedor a partir de información obtenida de los usuarios del servicio¹¹⁵. Así, el proveedor puede hacer uso de ellos, por ejemplo, para calcular recursos consumidos, monitorizar el rendimiento del servicio, o integrar conjuntos de datos como el *Big Data*. Sin embargo, nada impide que el usuario pueda reclamar su recuperación, especialmente respecto de aquellos que puedan aportar información personal, es decir, no anonimizados.

Dicho lo anterior, la heterogeneidad de servicios de computación en la nube obliga a matizar el sentido del deber de recuperación y portabilidad de los datos, puesto que existen servicios cuyo objeto principal no es el alojamiento de información remota, es decir, la capacidad de almacenamiento como prestación, sino, por ejemplo, otras funcionalidades del servicio que necesitan de datos introducidos por el cliente para ser operativas, como sucede con las redes sociales¹¹⁶. En este caso, aunque mantenemos nuestra postura sobre la existencia de un deber de restitución de los datos cuando el cliente así lo solicite del proveedor, la exigencia de un formato portable hacia otro proveedor puede suponer una carga excesivamente gravosa para el proveedor, siempre que no exista un estándar técnico a tal efecto, debido a incompatibilidades derivadas de la diferente configuración, uso y funcionalidad de cada red social. Igualmente, estos argumentos pueden ser extensibles entre servicios de computación en la nube particularmente diferentes

jurídicos de los contenidos alojados en la nube".

114 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).

115 Ver apartado "Datos generados por el proveedor o por terceros a partir de la información de los usuarios", en el capítulo "Aspectos jurídicos de los contenidos alojados en la nube".

116 La funcionalidad esencial de las redes sociales es la compartición de contenidos, aunque pueden ser utilizadas en la práctica como almacenamiento remoto. Conscientes de estos usos, muchas redes sociales ofrecen en su plataforma opciones para extraer copias de contenidos compartidos, y la posibilidad de eliminarlos. En los siguientes enlaces aparecen los pasos para recuperar información en las redes sociales *Facebook* y *Twitter*. Disponibles respectivamente en: <<http://www.solucionfacebook.com/2015/03/como-recuperar-contenido-eliminado-en.html>> y <<http://www.gadgetos.com/tutoriales/como-descargar-historial-mensajes-twitter/>>. [Fecha de consulta: 5 de abril de 2017].

CAPÍTULO SÉPTIMO

entre sí. En estos casos, lo más práctico para ambas partes será facilitar al cliente la recuperación de los datos en el mismo formato en el cual se migraron, o en un formato abierto y manejable cuando el primero haya podido quedar obsoleto, y que el propio cliente sea quien los exporte al formato que el nuevo entorno de nube requiera.

Tras la reciente actividad legislativa del ámbito europeo, probablemente esta tendencia contractual sufrirá cambios significativos. Por una parte, en lo que respecta a los datos de carácter personal, cuando sea aplicable el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)¹¹⁷. El Reglamento exige al responsable del tratamiento que informe al titular de los datos sobre el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar ese plazo. Así, cuando el proveedor *cloud* pueda considerarse encargado del tratamiento, deberá facilitar esta información a su empresario cliente, para que este pueda suministrarla al titular de los datos personales y así cumplir con las exigencias del artículo 13.2 del nuevo Reglamento 2016/679 General de Protección de Datos¹¹⁸. En casos de retenciones de datos personales, en virtud del Reglamento, el interesado podrá requerir al responsable la portabilidad o supresión de esos datos personales que se hallen alojados remotamente porque un empresario o profesional los haya transferido a entornos de nube para llevar a cabo el tratamiento automatizado de esos datos personales.

Cabe distinguir de nuevo entre datos de carácter personal y datos no

117 Al respecto, ver también las Directrices sobre el derecho a la portabilidad del Grupo de Trabajo del Artículo 29. Disponibles en: <<https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricesportabilidad.pdf>>. [Fecha de consulta: 22 de mayo de 2017]. Ver capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

118 Art. 13.2 del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos): "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: a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; (...)".

CAPÍTULO SÉPTIMO

personales. Ante los primeros, deberá estarse a la regulación del Reglamento General de Protección de Datos (cuando este sea aplicable) y al derecho del interesado a su recuperación, portabilidad y supresión, lo cual puede generar obligaciones legales tanto al cliente empresario en su papel de responsable, como al proveedor *cloud* como encargado del tratamiento sujeto a instrucciones del responsable¹¹⁹. Cuando la recuperación únicamente afecte a datos que no sean de carácter personal, cabe la posibilidad de que el proveedor configure la recuperación de los datos como un servicio añadido y no como una obligación principal vinculada al deber de custodia. Bajo esta panorámica, se encontraría dentro del deber de información, colaboración y buena fe del proveedor, en una fase previa a la suscripción del contrato, que el cliente tenga conocimiento de la existencia de este coste añadido, independientemente de que el servicio sea o no ofertado como gratuito, para que pueda valorar los riesgos y costes de tal extremo a la hora de elegir el servicio más adecuado. Igualmente, sería exigible la razonabilidad del coste que suponga la recuperación de los datos, para que no implique para el cliente una permanencia *de facto*, puesto que la no recuperación de los contenidos almacenados puede suponer para el cliente la dependencia del servicio prestado por ese concreto proveedor.

Asimismo, la reciente Propuesta de Directiva de Suministro de Contenidos Digitales prevé la recuperación de contenidos generados por el usuario u otros contenidos facilitados a los proveedores de suministro de contenidos digitales (si bien esta Propuesta de Directiva únicamente se aplicaría a usuarios consumidores), e insta a esos proveedores a utilizar formatos de datos de uso común, estándares, buenas prácticas y códigos de conducta¹²⁰. Con el fin de estimular la competencia del mercado único digital y facilitar los cambios de proveedor, la Propuesta de Directiva promueve la supresión de obstáculos, entre ellos los creados a través de condiciones contractuales y los ocasionados por la falta de medios que permitan al cliente

119 Para las cuestiones relacionadas con la portabilidad de datos de carácter personal, nos remitimos al capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

120 Considerando 28 de la Propuesta de Directiva de suministro de contenidos digitales: "Al aplicar lo dispuesto en la presente Directiva, los proveedores deben hacer uso de normas, especificaciones técnicas abiertas, buenas prácticas y códigos de conducta, incluso en relación con el formato de datos utilizados comúnmente para recuperar el contenido generado por el usuario o cualquier otro contenido facilitado por el consumidor, tanto si se han establecido a nivel internacional, a nivel europeo o a nivel de un sector industrial específico".

CAPÍTULO SÉPTIMO

(consumidor) a recuperar todos los datos generados por el uso del servicio digital¹²¹.

Si bien la Propuesta de Directiva no define los conceptos de recuperación y portabilidad de datos, en sus artículos 13 y 16, junto al derecho a resolver el contrato se recoge la obligación de facilitar al consumidor los medios técnicos para que pueda recuperar los datos generados por el uso del servicio de suministro de contenidos digitales y aquellos datos facilitados por el propio consumidor, sin cargo ni obstáculos, en un plazo razonable de tiempo y en un formato de uso habitual¹²². Deberemos estar a la aprobación definitiva de esta Propuesta y a su transposición en el Derecho español para poder hablar de un derecho a la recuperación de los contenidos del cliente consumidor de servicios de suministro digital. Lamentablemente, este derecho no es predicable, al menos por el momento, de aquellos clientes que no tienen la consideración legal de consumidor, como sucede con el pequeño empresario y el profesional independiente, y ello aunque, como se ha visto, su situación de desigualdad contractual ante el proveedor *cloud* sea equiparable a la del consumidor, y el valor de su información, igualmente apreciable.

Por el momento, los tribunales españoles no se han pronunciado sobre la recuperación y portabilidad de los datos en la computación en la nube, a diferencia de los tribunales franceses, quienes han reconocido la recuperación y portabilidad de los datos, combinación conocida también como reversibilidad en la computación en

121 Considerando 46 de la Propuesta de Directiva de suministro de contenidos digitales: "La competencia es un elemento importante para el buen funcionamiento del mercado único digital. Para estimular dicha competencia, los consumidores deben poder responder a ofertas competitivas y cambiar de proveedor. Con el fin de que esto funcione en la práctica, deben poder hacerlo sin verse limitados por obstáculos de índole legal, técnica o práctica, incluidas las condiciones contractuales o la falta de medios para recuperar todos los datos cargados por el consumidor, producidos por el consumidor mediante el uso de los contenidos digitales o generados a través del uso de los datos digitales por el consumidor. (...)".

122 Artículo 13.2.c) de la Propuesta de Directiva de suministro de contenidos digitales: "Cuando el consumidor resuelva el contrato: (...) el proveedor facilitará al consumidor los medios técnicos para recuperar todos los contenidos facilitados por el consumidor, así como cualquier otro dato producido o generado mediante el uso por el consumidor de los contenidos digitales, en la medida en que estos hayan sido retenidos por el proveedor. El consumidor tendrá derecho a recuperar los contenidos sin cargo alguno, sin mayores inconvenientes, en un plazo de tiempo razonable y con un formato de datos utilizado habitualmente". Artículo 16.4.b) de la Propuesta de Directiva de suministro de contenidos digitales: "Cuando el consumidor resuelva el contrato de conformidad con este artículo: [respecto del derecho a resolver los contratos de larga duración: (...), b) el proveedor facilitará al consumidor los medios técnicos para recuperar todos los contenidos facilitados por el consumidor, así como cualquier otro dato producido o generado mediante el uso por el consumidor de los contenidos digitales, en la medida en que estos haya sido retenidos por el proveedor. El consumidor tendrá derecho a recuperar los contenidos sin cargo alguno, sin mayores inconvenientes, en un plazo de tiempo razonable y con un formato de datos utilizado habitualmente, (...)".

CAPÍTULO SÉPTIMO

la nube, no solo fundamentada en la buena fe contractual, sino también como obligación principal del proveedor de servicios de computación en la nube¹²³.

5.2.4.- La asistencia al cliente durante el tránsito de los datos a un tercer proveedor. El plazo para la recuperación de los datos

Los contratos no suelen prever la asistencia en la transición a un nuevo

123 El *Tribunal de Grande Instance de Nanterre*, el 30 de noviembre de 2012 condenó al proveedor norteamericano de Software como Servicio Oracle a garantizar al partido político UMP la transferencia de los datos que esta había migrado a través de la herramienta de gestión de datos de clientes en la nube *Oracle CRM On Demand*, que el partido utilizaba para gestionar los datos de sus afiliados. El contrato establece un plazo de 60 días desde la fecha de extinción del contrato para que la empresa cliente pueda recuperar la información migrada. Cuando UMP quiso recuperar sus datos, se encontró con un error en la función del software que utilizaba que le impedía recuperar esos datos para así poder transmitirlos al nuevo proveedor. A la espera de que saliese al mercado la nueva versión, lo cual tardaría unos 10 meses en estar disponible al público, Oracle ofreció mantener el acceso al servicio de manera gratuita aunque el contrato hubiera expirado, hasta que pudieran haberse exportado el total de los datos almacenados, con lo cual estaba sometiendo a UMP a prorrogar el plazo del contrato suscrito. Oracle, por su parte, argumentó que el contrato no establecía que los servicios estarían exentos de errores de funcionamiento, y que por ello no había incumplido sus obligaciones contractuales. El juez consideró que esta medida era insuficiente para evitar los daños que pudiera sufrir UMP si se retrasaba su oportunidad de transferir los datos a un nuevo proveedor, que la ausencia de esta cláusula no podía beneficiar al proveedor predisponente, y que la reversibilidad es una de las obligaciones principales del proveedor *cloud*. Asimismo, fundamentó en la buena fe contractual y en la teoría general de los contratos (art. 1134 del Código civil francés) la equidad exigían que Oracle asegurase la reversibilidad del servicio en el caso de que un error aconteciera, y que esta obligación exigía no solo que UMP pudiera recuperar los datos migrados de sus afiliados, sino también de permitirle elegir un nuevo prestador y que pudiera reprendre con este la prestación (*"La société Oracle ne peut soutenir de bonne foi qu'elle ne manquerait pas à ses obligations contractuelles si elle ne permettait pas à l'UMP de bénéficier en temps utile de ses données pour permettre à son nouveau prestataire de les exploiter et d'être opérationnel dès la fin de sa propre prestation"*). Así, condenó a Oracle a abonar a UMP la cantidad de 5.000 € por día de retraso, y a facilitarle los medios técnicos que le permitan transferir los datos de los afiliados sin más retraso. Esta decisión judicial (una *"ordonnance de référé"*) destaca por la rapidez de su proceso y que en este caso se obtuvo en menos de tres semanas, y por ser directamente ejecutable, lo cual convierte en ideales este tipo de procesos rápidos para la resolución dinámica que demandan las cuestiones relacionadas con los servicios de computación en la nube y otros servicios de la sociedad de la información, y evitar así que estos asuntos se estancuen en largos procedimientos judiciales. Bajo nuestro punto de vista, si bien la condena dineraria es elevada, no deja de ser un buen precedente en cuanto a reconocer la existencia del derecho a recuperar los datos y a poder transferirlos a otro proveedor como obligación esencial del contrato, y que pueda servir de ejemplo asimismo la celeridad de la resolución. Información disponible en: <<http://www.eurocloud.fr/doc/varet-2014-03-11.pdf>>, <<http://www.dsidiiff.fr/telechargement/Actualites/Cloud-Computing-reversibilite.pdf>> y <<http://www.observatoire-fic.com/la-prevention-de-la-perte-des-donnees-de-lentreprise-a-lepreuve-du-droit/#sthash.jXHYhNw2.dpuf>>. [Fecha de consulta: 22 de mayo de 2017].

CAPÍTULO SÉPTIMO

proveedor de servicios *cloud* en relación a la transferencia de datos de un cliente, ni tampoco la colaboración directa con otros proveedores en dicha transición. Sin embargo, puede alegarse este deber de colaboración fundamentado en la buena fe contractual.

En el mismo sentido, hemos visto en el apartado anterior como el nuevo Reglamento de protección de datos europeo, 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, reconoce al titular de datos personales que, en ejercicio de su derecho a la portabilidad, y cuando sea posible técnicamente, que sus datos se transmitan directamente de responsable a responsable del tratamiento.

En aquellos casos en los cuales la naturaleza de los contenidos migrados no esté relacionada con la privacidad, el proveedor podría ser compelido a la asistencia en la transmisión de datos a un tercer proveedor, especialmente en aquellos casos que esa transmisión revista una notable dificultad técnica para el cliente, con base en los deberes de colaboración entre las partes y, cuando suponga una merma en la libertad del cliente para cambiar libremente de proveedor, en la buena fe contractual (art. 50 del Código de Comercio y 1258 del Código Civil¹²⁴).

Al igual que consideramos que esta idea de colaboración puede extrapolarse a los entornos de computación en la nube, y que, en la medida en que sea posible, el proveedor saliente debería asistir en la medida de sus posibilidades al cliente en su tránsito hacia un nuevo sistema *cloud*, cuando esta asistencia no sea posible, consideramos que, con fundamento en la colaboración entre las partes y la buena fe, deberá otorgarle un margen de tiempo suficiente para poder recuperar los datos y transferirlos por sí mismo antes de que se proceda a su borrado o se inhabilite la cuenta del cliente de manera definitiva.

Este margen de tiempo será establecido libremente por el proveedor, aunque sería recomendable que se tuviera en cuenta el volumen de datos involucrado, y la capacidad del cliente para recibirlo en sus propios sistemas, o, en su defecto, para

124 Art. 50 del Código de Comercio "Los contratos mercantiles, en todo lo relativo a sus requisitos, modificaciones, excepciones, interpretación y extinción y a la capacidad de los contratantes, se regirán, en todo lo que no se halle expresamente establecido en este Código o en las Leyes especiales, por las reglas generales del Derecho común". 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".

CAPÍTULO SÉPTIMO

buscar un proveedor alternativo que le permita continuar con una prestación similar¹²⁵. En relación al "tiempo razonable" durante el cual los datos estarán a disposición del cliente una vez extinguido el contrato, para que este pueda exportarlos y, en su caso, migrarlos a otro sistema *cloud*, la interpretación de esta expresión varía considerablemente dependiendo del prestador y del tipo de servicio. Así, se observan proveedores que estipulan un plazo determinado (generalmente, se establecen plazos que abarcan de 15 días a 6 meses)¹²⁶, proveedores que, a su discreción, determinarán el plazo una vez llegado el momento de la terminación, y otros que afirman que los datos se borrarán de manera inmediata una vez terminada la relación entre cliente y proveedor (mayormente, contratos gratuitos dirigidos a consumidores, sobre quienes recae, de manera obvia y aunque el contrato no lo especifique, la carga de realizar copias de seguridad preventivas de los contenidos, y quienes, por otro lado, podrán interesar la anulación de esta cláusula por abusividad¹²⁷⁾¹²⁸.

125 En los contratos examinados se encuentran diversidad de soluciones: desde contratos que no mencionan período alguno y afirman proceder al borrado inmediato de los datos una vez extinguida la relación, pasando por compromisos recogidos con términos del tipo "periodos comercialmente razonables", a plazos determinados, o hasta que el proveedor tenga confirmación de que el cliente efectivamente ha recuperado sus contenidos. Una vez pasado este tiempo, el proveedor cesa en su compromiso de mantener el acceso del cliente a la prestación y, en ocasiones, afirma proceder a su borrado.

126 Sirva de referencia, para la comparación entre contratos *cloud*, BRADSHAW, S; MILLARD, C; WALDEN, I, "Standard contracts for Cloud Services", *Cloud Computing Law*, (Coord. Christopher Millard), 1ª edición, Oxford, 2013, pág. 52.

127 En especial, por ser una cláusula "(...)" que le faculden [al proveedor] a resolver los contratos de duración indefinida en un plazo desproporcionadamente breve o sin previa notificación con antelación razonable" (art. 85.4 TRLGDCU), "la imposición de cualquier otra renuncia o limitación de los derechos del consumidor y usuario" (art. 86.7 TRLGDCU) y "(...)" que impongan obstáculos onerosos o desproporcionados para el ejercicio de los derechos reconocidos al consumidor y usuario en el contrato, en particular en los contratos de prestación de servicios o suministro de productos de tracto sucesivo o continuado, (...) la renuncia o el establecimiento de limitaciones que excluyan u obstaculicen el derecho del consumidor a poner fin a estos contratos" (art. 87.6 TRLGDCU).

128 A continuación, varios ejemplos de cláusulas de recuperación de datos. Condiciones generales del software como servicio (SaaS) *Google G-Suite* [en línea]: "En caso de rescisión del presente acuerdo (...), ii) Google proporcionará al cliente acceso a los datos del cliente, así como la capacidad de exportarlos, durante un periodo de tiempo comercialmente razonable y a los precios de Google vigentes en ese momento para los servicios aplicables, iii) tras un periodo de tiempo comercialmente razonable, Google eliminará los datos del cliente mediante la supresión de redireccionamientos que hagan referencia a estos en los servidores activos de [el proveedor] y sobrescribiéndolos conforme transcurra el tiempo, iv) cada una de las partes aplicará de inmediato todos los esfuerzos comercialmente razonables para devolver o destruir cualquier otra Información confidencial de la otra parte, si así se solicita. (...)". Condiciones de uso del software como servicio (SaaS) de almacenamiento remoto de datos Box [en línea]: "Aparte de otras disposiciones sobre terminación, si su cuenta no está sujeta en ese momento a un plan de suscripción de pago

CAPÍTULO SÉPTIMO

Por nuestra parte, consideramos que el prestador *cloud* es quien es consciente del grado de dificultad que pueda suponer la recuperación de los datos y la transmisión de esos datos a otros sistemas, o de la facilidad de encontrar un proveedor que oferte servicios similares. Igualmente, es quien tiene más conocimiento del sector y sus usos para intuir el tiempo que puede tardarse hasta que estas operaciones hayan tenido lugar de manera satisfactoria y el cliente pueda volver a disfrutar de un servicio equivalente plenamente operativo.

Por ello, opinamos que puede invocarse el principio de buena fe contractual en aquellos casos en los cuales el margen de tiempo ofrecido al cliente sea injustificadamente breve, sobre todo en aquellos casos en los cuales el cliente sea un empresario que deba someterse a procesos especialmente complicados (ya sea por el tipo de servicio prestado, por el volumen o naturaleza de los contenidos migrados o por otras razones) y que durante este tránsito vea mermada la operativa habitual que sustenta su actividad económica. Del mismo modo, cuando no se establezca tiempo para proceder a la recuperación de esos datos, pueden servir de referencia los usos del sector (art. 2 del Código de Comercio¹²⁹).

6.-LA PRESERVACIÓN DE LOS CONTENIDOS Y SU BORRADO UNA VEZ EXTINGUIDA LA RELACIÓN CONTRACTUAL

Tras haber analizado diferentes cuestiones jurídicas en relación a si el proveedor puede retener los datos del cliente e impedir que los recupere o transfiera a otro proveedor, a continuación nos plantearemos si el proveedor puede conservar copias de los contenidos del cliente una vez que el proceso de recuperación de la información ha concluido de manera exitosa. Por último, realizaremos varias consideraciones en cuanto a la existencia de una obligación del proveedor de

concertado con nosotros, podremos, a nuestra entera discreción, dar por terminada su cuenta si: a) no realiza ninguna actividad en la misma durante los (30) días siguientes a su alta como Usuario registrado, o b) no realiza ninguna actividad en la misma durante ciento veinte (120) días consecutivos. En caso de terminación de su cuenta en esas circunstancias, el Contenido que pueda tener almacenado se perderá". Disponibles respectivamente en: <https://gsuite.google.com/intl/es/terms/2013/1/premier_terms.html>. y <<https://www.box.com/legal/termservice/ES/>>. [Fecha de consulta: 4 de abril de 2017].

129 Art. 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".

CAPÍTULO SÉPTIMO

eliminar todas las copias de los contenidos del cliente remanentes en los diferentes centros de datos que están bajo su control.

Como es sabido, forma parte de la arquitectura de nube pública la compartición de recursos entre diferentes usuarios, así como el replicado múltiple de datos con diferentes finalidades, como la de facilitar su recuperación en caso de que se produzcan incidentes de seguridad. Como consecuencia de ello, la eliminación definitiva de los contenidos de un determinado cliente puede suponer complicaciones técnicas y costes para el proveedor. Para abordar este tema de manera adecuada, será necesario entender en qué forma tiene lugar el proceso de borrado y destrucción de datos dentro de entornos de la nube, si puede tener implicaciones en el ámbito del contrato y cuál es la normativa actual que pueda resultar aplicable. En este último aspecto, resulta de especial trascendencia la regulación en materia de privacidad.

6.1.- La preservación de los contenidos del cliente tras finalizar la prestación

La información que maneja una empresa puede tener datos sensibles, como aquellos que tengan valor comercial o resulten estratégicos para el negocio, o que sean de carácter personal. Anteriormente hemos estudiado la retención de datos por el proveedor cuando el servicio quedaba en suspensión por diversos motivos (impago, infracción de políticas de uso adecuado, etc.), pero en esos momentos la relación jurídica seguía todavía vigente. Por ello, la gestión de esa información una vez finalizada su vida útil es igualmente de suma importancia para la empresa que los ha generado¹³⁰.

El empresario cliente de servicios *cloud* debe interesarse, antes de suscribir el contrato, por la potencial existencia de condiciones generales que habiliten la cesión del uso de datos empresariales (que carezcan de la calificación de dato personal) al proveedor *cloud*, incluso una vez terminada la relación contractual, como hemos

130 Al respecto, el instituto Nacional de Ciberseguridad INCIBE ha elaborado una Guía sobre borrado seguro de la información. Disponible en: <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_meta0.pdf>. [Fecha de consulta: 22 de mayo de 2017].

CAPÍTULO SÉPTIMO

observado en anteriores capítulos (por ejemplo, cesiones de derechos de propiedad intelectual)¹³¹. Del mismo modo, deberá tener especial precaución en relación al tratamiento de estos datos dentro de la nube, y a su destino una vez finalizada la relación jurídica¹³².

A continuación, vuelve a ser necesario distinguir entre datos de carácter personal y datos no personales. Con el nuevo Reglamento 2016/679 General de Protección de Datos, se pretende limitar el tratamiento de datos personales a los fines para los que se recabaron, utilizando dos medidas para conseguirlo¹³³. Una de ellas consiste en exigir al responsable del tratamiento que establezca y revise periódicamente el plazo de conservación de estos datos, y que proceda a su supresión inmediata cuando ya no sea necesario mantenerlos, siempre y cuando la normativa europea o nacional no obligue a conservarlos. En cumplimiento de esta obligación, el responsable del tratamiento (en este caso, nos referiríamos al empresario-cliente de servicios *cloud*) deberá dar traslado de las instrucciones pertinentes al encargado (proveedor *cloud*), y este deberá proceder a devolver, suprimir o conservar esos datos personales de acuerdo con tales instrucciones, con lo establecido en el contrato entre ambos y en la legislación aplicable¹³⁴. Igualmente, el responsable deberá informar de este plazo cuando obtenga estos datos del interesado, en el momento en que los recabe, para garantizar "un tratamiento de datos leal y transparente" (art. 13.2.a) del Reglamento 2016/679)¹³⁵.

La otra medida utilizada por el Reglamento 2016/679 para limitar la conservación de los datos consiste en restringir el uso de los datos personales cuando

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

132 Dedicaremos posteriores apartados de este capítulo al estudio de este aspecto.

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

134 Esta obligación se recoge en el art. 28.3.g) del Reglamento 2016/679: "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: (...) 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; (...)".

135 Art. 13.2 del Reglamento 2016/679: "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: a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;(…)".

CAPÍTULO SÉPTIMO

pueden sustituirse por otros datos no personales que cumplan la misma función, es decir, que los datos personales solo puedan conservarse en la medida en la que la finalidad del tratamiento no pueda llevarse a cabo con otros mecanismos que eviten el manejo de tal información¹³⁶. La finalidad del tratamiento de datos personales debe ser lícita de acuerdo con la normativa de la Unión Europea y de los Estados miembros, la cual también puede establecer límites a esa finalidad y plazos de conservación de los datos¹³⁷.

En cuanto a los plazos que permitan la conservación de los datos personales, estos son ponderables atendiendo a los fines del tratamiento de esos datos (de acuerdo con el actual artículo 4 de la LOPD), y a si se permite con ellos la identificación del interesado,(nuevo artículo 5 del Reglamento 2016/679¹³⁸.

136 Esta idea aparece ya recogida de manera general en la exposición de motivos del Reglamento 2016/679. "Considerando 39. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica".

137 Así lo reconoce el Considerando 45 del Reglamento 2016/679: "La finalidad del tratamiento también debe determinarse en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal", y su artículo 6.3: "La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por: a) el Derecho de la Unión, o b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento. (...) Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, (...)".

138 Al respecto, el art. 4 de la Ley Orgánica de protección de datos establece la necesidad de cancelar esos datos cuando se haya cumplido la finalidad del tratamiento, salvo algunas excepciones: "Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos". Por otra parte, el art. 5.1.e) del Reglamento 2016/679 permite ampliar este plazo cuando así lo requieran otros intereses: "Los datos personales serán: (...) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos

CAPÍTULO SÉPTIMO

El cliente pequeño empresario deberá asegurarse, como responsable, de que el proveedor procesará los datos personales mediante alguna técnica lo suficientemente segura para entender protegidos los derechos de los individuos interesados, regulando previamente estos aspectos relativos a los procesos de seguridad de los datos a través del contrato entre responsable y encargado del tratamiento¹³⁹.

Respecto de datos que no tengan la consideración de dato personal, la Propuesta de Directiva de suministro de contenidos digitales establece, respecto del consumidor, que el proveedor adoptará las medidas que podrían esperarse para abstenerse de utilizar datos facilitados por el cliente, sean o no de carácter personal (art. 13.b¹⁴⁰). Este artículo, a nuestro parecer, se redacta en unos términos no suficientemente tajantes, permitiendo al proveedor ciertos usos de los contenidos migrados por el usuario, y sin pronunciarse sobre otras cuestiones que a nuestro parecer son importantes, como aquellas relacionadas con la propiedad intelectual de los datos del usuario. Por supuesto, es importante remarcar que esta norma se restringe al ámbito de las relaciones con consumidores, con lo cual el pequeño

personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»).

139 Cuando los datos en manos del proveedor *cloud* tienen carácter de dato personal, y han sido facilitados directamente por el particular suscriptor del servicio y titular de esos datos, el proveedor, como responsable del tratamiento, podrá tratar esos datos siempre que, como es presumible, haya obtenido a través de las condiciones generales el consentimiento legal exigido. En estas condiciones, es posible que el titular habilite al proveedor a hacer uso con finalidades ajenas a la prestación del servicio, incluso tras haberse extinguido la relación contractual entre ambos, por ejemplo, por fines relacionados con estadísticas, publicidad o Big Data. Para evitar esas utilidades una vez el contrato se ha extinguido, el cliente titular podrá hacer uso de su derecho de cancelación o supresión, como veremos en este mismo capítulo.

140 Art. 13.b) de la Propuesta de Directiva de suministro de contenidos digitales: "Cuando el consumidor resuelva el contrato: (...) el proveedor adoptará todas las medidas que podrían esperarse para abstenerse de utilizar las contraprestaciones no dinerarias que el consumidor haya facilitado a cambio de los contenidos digitales, así como cualesquiera otros datos recogidos por el proveedor en relación con el suministro de los contenidos digitales, incluido cualquier contenido facilitado por el consumidor, a excepción del contenido que haya sido generado conjuntamente por el consumidor y otras personas que continúen haciendo uso del contenido, (...)". Respecto de la resolución de los contratos de suministro de contenidos digitales de larga duración, art. 16.3.c) se establece una disposición similar: "el proveedor adoptará todas las medidas que podrían esperarse para abstenerse de utilizar contraprestaciones no dinerarias que el consumidor haya facilitado a cambio de los contenidos digitales, así como cualesquiera otros datos recogidos por el proveedor en relación con el suministro de los contenidos digitales, incluido cualquier contenido facilitado por el consumidor".

CAPÍTULO SÉPTIMO

empresario vuelve a quedar, al menos en principio, fuera de su cobertura.

La reserva de información en favor del proveedor puede colisionar con el interés legítimo del empresario cliente de que no queden datos remanentes en los sistemas de nube una vez que la relación jurídica se haya extinguido, es decir, con su expectativa de que se eliminen de la nube. Sin embargo, por el momento y a falta de normativa específica para contratos entre empresas, deberemos estar a lo establecido al respecto en las condiciones contractuales suscritas.

Independientemente de lo que establezca el contrato, y como hemos manifestado en capítulos anteriores, consideramos que forma parte de las obligaciones contractuales del proveedor la custodia de los datos y el ofrecer las máximas garantías en relación a su seguridad, esto es, que los datos sean confidenciales, estén accesibles al cliente y se conserven de manera íntegra¹⁴¹. Esta obligación de custodia se mantiene, como es evidente, durante todo el período de vigencia de la relación contractual. Una vez extinguido el vínculo jurídico entre ambas partes, el proveedor está obligado a posibilitar la recuperación de esos contenidos al cliente con todas sus cualidades, obligación que sigue formando parte esencial de su posición jurídica de prestador del servicio *cloud*, en cuanto a la restitución de aquello custodiado.

Sin embargo, hemos manifestado que, por diversas razones, el proveedor puede quedar habilitado para conservar parte de la información en sus sistemas, con lo cual podemos deducir de la naturaleza del contrato que deberá mantenerse la seguridad de esos datos en la medida en que durante su custodia no se produzcan perjuicios al cliente o a terceros. Así, continúa persistiendo en el tiempo el deber de su custodia segura como un deber de liquidación, es decir, aquellos deberes derivados de "la necesidad de liquidar sus resultados [es decir, los resultados de la relación obligatoria] o la situación que se encuentra pendiente"¹⁴². Pensamos que, aunque la relación obligatoria entre proveedor y cliente ha llegado a su fin, perdurará para el proveedor la obligación de custodia derivada de aquellos datos remanentes en los sistemas que, por una razón u otra, el proveedor conserva, puesto que tal preservación trae su causa en la relación jurídica ahora ya extinguida.

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

142 DIEZ-PICAZO, *Fundamentos del Derecho Civil Patrimonial, Vol. II: Las relaciones obligatorias*, Navarra, 2008, Sexta edición, pág. 1084.

CAPÍTULO SÉPTIMO

A continuación, nos detendremos en las diferentes técnicas de borrado de datos y en las garantías que ofrecen al cliente *cloud*, así como en otras medidas jurídicas y técnicas que pueden combinarse con el borrado como medidas de salvaguarda de intereses.

6.2.-Las técnicas de borrado de contenidos en la computación en la nube y sus garantías

En sistemas informáticos, y entre ellos, en entornos de computación en la nube, existen diferentes niveles de eficiencia en la eliminación de información digital. El nivel de eficiencia de los mecanismos de borrado suele ser proporcional a su coste: cuantas más garantías ofrece al cliente, más coste implica para el proveedor de almacenamiento. Los prestadores de servicios *cloud*, por tanto, serán reacios a proporcionar los mecanismos de borrado más costosos a cualesquiera clientes de sus servicios, reservándolos para aquellos casos en los que lo consideren estrictamente necesario, y siempre intentarán trasladar los costes al cliente para obtener el mayor rendimiento económico en cada transacción.

Por otro lado, en relación a datos de carácter personal, existen otras técnicas diferentes al borrado que pueden servir a las finalidades perseguidas por ambas partes. Así, al proveedor pueden serle útiles datos que ha generado el cliente para realizar monitorizaciones del servicio, estadísticas o que formen parte de bases de datos y del *Big Data*. Por contrapartida, tras el uso de técnicas como la anonimización, el titular de los datos mantiene protegida su privacidad al desvincularse esos datos de su identidad, y el cliente responsable deja de serlo por ese tratamiento de datos cuando dejan de tener carácter de datos personales.

A continuación, distinguiremos entre el borrado de datos y otras técnicas que se aplican a datos de carácter personal.

6.2.1.- Los diferentes niveles de borrado de los datos

La criticidad de los datos afectados se configura como un factor determinante a la hora de determinar el mecanismo de borrado más adecuado. El procedimiento más seguro es aquel que destruye o inutiliza el *hardware* de almacenamiento de los

CAPÍTULO SÉPTIMO

datos (por ejemplo, el disco duro que los contiene), puesto que al desintegrarse completamente todos los soporte físicos que los sustentan, los contenidos digitales se vuelven prácticamente irrecuperables, incluso para expertos informáticos.

Pero, como podemos deducir, la destrucción del *hardware* no es un sistema de borrado comercialmente viable para la mayoría de proveedores, puesto que pretenden seguir utilizando el *hardware* que han adquirido, para así amortizar su inversión. Difícilmente encontraremos un proveedor de entornos de nube pública que se comprometa a destruir los soportes físicos para proceder al borrado del cliente, puesto que entrañaría complicaciones técnicas y cargas económicas que no permitirían sustentar un modelo de negocio basado en servicios de bajo coste y en la suscripción de capacidades de manera masificada.

Partiendo de la misma idea de nube pública como modelo de servicio, cualquier empresario que maneje datos digitales que sean tan sensibles y confidenciales como para exigir la destrucción de los soportes físicos que se custodian, debería replantearse la posibilidad de migrarlos a entornos más cerrados y controlables, como pudiera ser una nube privada o conservarlos en servidores propios, debiendo entenderse este planteamiento, a nuestro modo de ver, como parte de su deber de diligencia empresarial.

En entornos de nube pública, como hemos mencionado, no suele ofrecerse al cliente el mecanismo de borrado consistente en destruir el soporte físico que almacena los contenidos digitales. Generalmente, cuando se habla de borrar un conjunto de contenidos se hace referencia al borrado común, es decir, el sistema identifica el espacio que ocupaban esos contenidos como espacio libre, con lo cual, por una parte, esos datos digitales dejan de estar plenamente accesibles y, por otra, ese espacio puede ser sobrescrito por datos nuevos, que gradualmente se irán almacenando en ese mismo dispositivo *hardware*¹⁴³. Los métodos de comando de

143 Para una mejor comprensión del proceso de borrado en sistemas *cloud*, podemos realizar una comparación en el ámbito de la informática doméstica, mediante un ejemplo pensado para usuarios de sistemas operativos *Windows*. El hecho de que nosotros demos la orden de eliminar un archivo o carpeta de nuestro disco duro local no significa que este archivo quede totalmente inaccesible, irrecuperable y destruido de manera inmediata. De hecho, ese archivo o carpeta que hemos decidido eliminar se ha renombrado y almacenado en la llamada "papelera de reciclaje", y podremos restaurarlo de nuevo, si así lo deseamos. Aun cuando este archivo sea eliminado de manera permanente a través de los comandos adecuados sin almacenarse previamente en la "papelera de reciclaje", existen mecanismos de reversión que permiten recuperar datos de soportes

CAPÍTULO SÉPTIMO

borrado del sistema operativo o el formateo de alto nivel de dispositivos no se consideran técnicas de borrado seguro¹⁴⁴.

El borrado mediante destrucción de dispositivos o desmagnetización resulta más eficaz que el borrado por sobreescritura en la que la propia herramienta de borrado se encarga de sobrescribir datos con caracteres distintos que imposibilitan su recuperación. Consideramos que existe la posibilidad de que, a través de técnicas de informática forense, se pueda rescatar y reconstruir parte de esos datos, dado que nunca llegan a desaparecer del soporte de almacenamiento que los contiene y que permanece íntegro. No obstante, cuantas más veces se hayan sobrescrito los datos inicialmente borrados, más dificultosa será su recuperación, pudiendo llegarse a un punto en el cual esa recuperación sea inviable¹⁴⁵.

Por último, en cuanto a la prueba de la eficacia del borrado, cabe decir que la sobreescritura de datos permite obtener una garantía documental del proceso, mientras que otros mecanismos de borrado o destrucción suponen dificultades para certificar la operación.

6.2.2.- Algunas medidas relacionadas con el borrado: la cláusula de confidencialidad, la anonimización y la seudonimización

Como hemos avanzado, existen medidas que pueden relacionarse con el borrado de los datos del cliente utilizadas por los proveedores, y para su adecuada

que siguen activos. También permanecerán intactas todas aquellas copias de los datos que tengamos en otras particiones o soportes extraíbles de almacenamiento (discos duros externos, memorias USB, etc.). Un sistema similar a la papelera de reciclaje se pone a disposición del usuario del software como servicio (SaaS) de almacenamiento *Dropbox*, tal y como puede comprobarse en la ayuda del proceso de recuperación de datos en su sitio web. Disponible en: <https://www.dropbox.com/es_ES/help/969>. [Fecha de consulta: 22 de mayo de 2017].

144 Así lo afirma el Instituto Nacional de Ciberseguridad INCIBE (antes INTECO), adscrito al Ministerio de Industria, Energía y Turismo, en su *Guía sobre borrado seguro de la información* [en línea], especialmente dirigida a empresarios. Si bien en esta guía se mencionan los diferentes sistemas de destrucción de la información, y se determinan las ventajas e inconvenientes, por ejemplo, de la destrucción física o de la sobreescritura progresiva, no se hace especial referencia a los sistemas de almacenamiento en la nube. <https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_borrado_seguro_metad_0.pdf>. [Fecha de consulta: 22 de mayo de 2017].

145 Así, el formateo rápido de un disco duro puede permitir, en muchas ocasiones, recuperar datos que aparentemente se habían eliminado. Existen formateos más seguros, como el llamado formateo de baja densidad con sobreescritura, que sobrescribe datos aleatorios o ceros sobre la superficie del dispositivo (el cero, en sistema binario, representa un vacío de información).

CAPÍTULO SÉPTIMO

adopción, consideramos que es relevante la finalidad que persigue el cliente pequeño empresario en relación al borrado de aquellos datos que dejan de ser necesarios tras finalizar la relación jurídica. En algunos casos, la respuesta a esta cuestión estará íntimamente relacionada con que se impida acceder a quienes no estuvieran autorizados, con el fin de mantener su confidencialidad e integridad. En otros casos, la finalidad que se persigue con el borrado estará conectada con los derechos de titulares de datos personales en cuanto a aspectos de la privacidad contenidos en cierta información. A continuación, estudiaremos algunas medidas relacionadas con el borrado de datos que permitan su conservación, aunque para ello será necesario distinguir, de nuevo, los datos personales del resto de contenidos de naturaleza no relacionada con la privacidad. Asimismo, queremos aclarar que el hecho de relacionar estas opciones (cláusula de confidencialidad, seudonimización o anonimización) con el borrado no implica que tengan la misma efectividad ni consecuencias jurídicas que el borrado definitivo de datos, sino que se ofrecen a modo de medidas complementarias que permiten mantener la confidencialidad y evitar usos posteriores no autorizados de los datos del cliente.

a) La cláusula de confidencialidad

La información que no sea referente a datos personales que quede remanente en sistemas del proveedor *cloud*, y siga siendo relevante para el negocio del cliente (secretos empresariales, datos sobre ventas, información financiera, proyectos de I + D, datos relacionados con patentes o derechos de propiedad intelectual, etc.), puede protegerse con una cláusula de confidencialidad adecuadamente redactada en las condiciones generales, y que habilite al cliente perjudicado a interponer la acción pertinente¹⁴⁶. No obstante, los proveedores suelen ser reacios a incluir este tipo de

146 Cláusula de confidencialidad en las condiciones de Oracle: "Información Confidencial (no revelación) Por virtud del presente Acuerdo las partes pueden tener acceso a información confidencial de las mismas (en adelante "información confidencial"). La información confidencial quedará limitada a los Programas, a los términos y las tarifas pagaderas bajo el presente acuerdo, así como a toda otra información claramente identificada como confidencial. La información confidencial de una parte no incluirá información la cual: (a) es o comience a ser parte del dominio público por causa distinta de la acción u omisión de la otra parte, o (b) estuviera en posesión legítima de la otra parte antes de la revelación y no hubiera sido obtenida por la otra parte directa o indirectamente de la parte reveladora o (c) es legítimamente revelada a la otra parte por una tercera parte sin restricciones en la revelación o (d) es independientemente desarrollada por la otra parte. Cada uno de nosotros consiente en mantener la confidencialidad de la respectiva información confidencial de la otra durante un período de tres años a contar desde la fecha de su revelación. Asimismo, cada uno de nosotros acuerda revelar la información confidencial tan solo a aquellos empleados u agentes que necesiten acceder a la misma para el desarrollo del presente acuerdo y que necesiten protegerla frente a revelaciones no autorizadas. Nada de lo aquí establecido impedirá a cualquiera de las partes el revelar los

CAPÍTULO SÉPTIMO

cláusulas en sus acuerdos, especialmente en lo que respecta a la confidencialidad de la información facilitada por el cliente.

A falta de esta cláusula en las condiciones generales, o ante una limitación o exoneración de responsabilidad sobre ese aspecto que haya sido aceptada por el cliente empresario, consideramos que este cliente podría igualmente reclamar ante los tribunales una compensación, por ser la vulneración de la confidencialidad un incumplimiento de las obligaciones inherentes a la naturaleza del propio contrato de servicios de computación en la nube: el deber de custodia de los datos que se le presume al proveedor *cloud* como parte de su *lex artis*¹⁴⁷. El proveedor, en su caso, debería responder de tal infracción ante el perjudicado, y eventualmente, repetir contra aquellas personas que, bajo su responsabilidad, tuvieron acceso a tal información y quienes efectivamente decidieron y realizaron la filtración o uso indebido (empleados, subproveedores, etc.).

b) La anonimización de información personal

En cuanto a los datos personales, también existen otros mecanismos que pueden añadir garantías y complementar el borrado. Algunos de ellos garantizan la desvinculación de esos datos personales con la identidad de la persona física a quien conciernen, como las técnicas de anonimización. Otras dificultan la lectura inteligible de la información, como las técnicas de cifrado, o precisan de información accesoria para conectar la información personal y la persona física a la cual hacen referencia, también llamadas seudonimización. A continuación, veamos en qué consisten y en qué forma aparecen recogidas por la normativa en materia de protección de datos de carácter personal.

El Grupo de Trabajo del Artículo 29 definió en su Dictamen 5/2014 sobre técnicas de anonimización que esta técnica "es el resultado de un tratamiento de los datos personales realizado para evitar de forma irreversible su identificación", y posteriormente describe sus principales técnicas: la aleatorización y la generalización, que a menudo se combinan con otras técnicas para ofrecer más garantías¹⁴⁸. Tras delimitar su contenido, el

términos o precios del presente acuerdo o de los pedidos remitidos con sujeción a éste acuerdo en cualquier procedimiento legal que pudiera plantearse en relación o conexión con este acuerdo".

147 Si el suscriptor del servicio de computación en la nube es un consumidor, podría considerarse abusiva una cláusula que, ante la infracción del deber de confidencialidad, exima al proveedor de compensarle o entablar acciones legales.

148 En 2014, el Grupo de Trabajo del Artículo 29 elaboró un dictamen sobre las diferentes

CAPÍTULO SÉPTIMO

mismo Dictamen distingue la anonimización de la seudonimización, puesto que la segunda consiste en la sustitución de un atributo por otro en un registro¹⁴⁹. Concluyó el Grupo de Trabajo en este dictamen que las técnicas de anonimización pueden garantizar en gran parte la privacidad, aunque su eficiencia dependerá del contexto y de la finalidad con los cuales se utilicen estas técnicas, puesto que la legislación europea no establece ninguna técnica de manera preceptiva¹⁵⁰

No obstante, a pesar de las precisiones terminológicas (a nuestro parecer, acertadas), efectuadas en su momento por el Grupo de Trabajo del Artículo 29 en el mencionado Dictamen sobre técnicas de anonimización, sorprende como el artículo 4.5 del Reglamento 2016/679, que recoge las definiciones a efectos de la propia norma, únicamente recoja el concepto de "seudonimización", al que otorga de un significado diferente al recogido previamente por el Grupo de Trabajo del Artículo 29: "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".

A nuestro parecer, este concepto engloba las técnicas de anonimización y seudonimización anteriormente definidas por el Grupo de Trabajo, y afirma que pueden formar parte del proceso del tratamiento de datos de carácter personal. La definición de seudonimización recogida en el Reglamento General de Protección de Datos también enfatiza la necesidad de información adicional para conseguir asociar esos datos con una identidad, y exige que la obtención de esta información añadida no debe ser obvia o sencilla. Para entender que se ha llevado a cabo ese proceso de seudonimización, los datos personales se habrán sometido a medidas técnicas u

técnicas de anonimización, reconociendo su valor potencial y estableciendo las ventajas y riesgos entre ellas, con el fin de que pueda adoptarse el proceso más adecuado en cada contexto. El Dictamen 5/2014 sobre técnicas de anonimización (WP216) define la aleatorización como "una familia de técnicas que modifican la veracidad de los datos a fin de eliminar el estrecho vínculo existente entre los mismos y la persona", ya que "si los datos se hacen lo suficientemente ambiguos, no podrán remitir a una persona concreta", y la generalización como un enfoque que "generaliza o diluye los atributos de los interesados modificando las respectivas escalas u órdenes de magnitud (por ejemplo, sustituyendo una ciudad por una región, o una semana por un mes)", págs. 13,14.

149 Por ejemplo, en substituir un dato con un número aleatorio que se le asocie a través de una función Hash. Grupo de Trabajo del Artículo 29, Dictamen 5/2014, pág. 24.

150 Para más información sobre la seudonimización y el encriptado, nos remitimos a HON, W. Kuan; MILLARD, C; WALDEN, Ian; "What is Regulated as Personal Data in Clouds?", *Cloud Computing Law*, (Coord. Christopher Millard), 1ª edición, Oxford, 2013, págs. 169 y ss.

CAPÍTULO SÉPTIMO

organizativas que dificultarían al máximo el enlace entre los datos y la persona física a quien se refieren. Como última puntualización, queremos poner de relieve que el propio Reglamento General de Protección de Datos parece reconocer que la seudonimización implica mecanismos no infalibles y que su promoción se realiza con el fin de reducir los riesgos de los interesados, pero no como medida totalmente garantista, como recogen sus considerandos 26 y 28¹⁵¹.

El concepto del Reglamento General de Protección de Datos deberá ser el concepto que se adopte como referencia legal de "seudonimización", en beneficio de una interpretación homogénea de la norma en todo su ámbito territorial de aplicación, aunque, en nuestra opinión, y con el fin de conseguir una mayor adecuación entre los significados de este concepto desde los puntos de vista de las disciplinas informática y legal, en nuestra opinión hubiera sido preferible mantener la distinción realizada por el Grupo de Trabajo.

Por otra parte, la definición de "dato personal" que realiza el Reglamento General de Protección de Datos hace referencia a la posibilidad directa o indirecta de identificar a una persona física a través de ciertos datos, los cuales tendrán la consideración de datos personales¹⁵². *A sensu contrario*, no tendrán la consideración de datos personales aquellos datos que, aunque hayan sido generados o se refieran a

151 Esta idea puede deducirse de los considerandos 26 ("Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos") y 28 del Reglamento 2016/679 General de Protección de Datos ("La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos") y de la definición del concepto recogida por el artículo 4.5 del Reglamento General de Protección de Datos.

152 Artículo 4.1 del Reglamento 2016/679 General de Protección de Datos: "«datos personales»: 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 en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona; (...)".

CAPÍTULO SÉPTIMO

una persona física, la identidad de esta persona no pueda deducirse a través de investigaciones posteriores de esa información que se ha proporcionado sobre ella¹⁵³. Por ello, quedará fuera del ámbito de la protección de datos personales aquella información referente a personas pero que haya sufrido un proceso de anonimización que ofrezca garantías sobre su irreversibilidad, pudiendo calificarse como información anónima, y, consecuentemente, como se ha dicho, quedando fuera del alcance del Reglamento General de Protección de Datos (Considerando 26)¹⁵⁴.

153 Como dice el considerando 26 del Reglamento: "Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación". La Ley Orgánica de Protección de Datos define, en la letra o) su artículo 5, como persona identificable a "toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social", y afirma a continuación que "una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados". En el mismo sentido opera la interpretación de datos anónimos realizada por el Grupo de Trabajo del Artículo 29 en su Opinión 4/2007 sobre el concepto de datos personales, pág. 21 [en línea]. Disponible en: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>. [Fecha de consulta: 17 de febrero de 2017].

154 Al igual que existen procesos de anonimización, se están desarrollando herramientas tecnológicas con el fin de revertir este proceso y poder identificar a las personas físicas a partir de la información proporcionada. Por esta razón, tampoco puede asumirse que la anonimización sea un mecanismo infalible e irreversible que ofrece las máximas garantías en relación a la privacidad y a la no necesidad de borrar o destruir datos personales. Por cuestiones objeto de este trabajo, no entraremos a analizar las consecuencias jurídicas que alcanzan a quienes realizan tales actividades, consecuencias que, por otra parte, suponen un nuevo reto para los organismos reguladores. Lo que sí podemos afirmar es que, en aquellos casos en los que el mecanismo utilizado para la anonimización no es considerado suficientemente robusto (es decir, que su reversión requiera de considerable complejidad técnica), los datos afectados pueden llegar a considerarse datos personales al ser identificable la persona a la cual hacen referencia. En este caso, por tanto, resultaría de aplicación la normativa sobre privacidad a todos sus efectos. Para un estudio más detallado sobre la anonimización y sus riesgos, nos remitimos al Dictamen 5/2014 del Grupo de Trabajo del Artículo 29, sobre técnicas de anonimización [en línea], <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf>; y a OHM, Paul, "Broken promises of privacy: responding to the surprising failure to anonymization", *UCLA Law Review*, Vol. 57, págs. 1701-2010, 2009. Disponible en línea en: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006>. [Fecha de consulta: 17 de febrero de 2017].

CAPÍTULO SÉPTIMO

c) La seudonimización de información personal

Hemos observado en el apartado anterior que el Reglamento General de Protección de datos recoge en su artículo 4.5 una definición de seudonimización no coincidente con la efectuada anteriormente por el Grupo de Trabajo del Artículo 29, y hemos puesto de relieve las diferencias existentes entre ambos conceptos.

Siguiendo con el concepto acuñado por el Grupo de Trabajo del Artículo 29, la seudonimización puede descomponerse en diferentes procesos técnicos, cada uno con distintas aplicaciones y distinto nivel de garantías en cuanto a su reversibilidad. Entre estos procesos, destacan ciertos tipos de cifrado por claves y la aplicación de algoritmos que tienen como resultado una información con caracteres diferentes¹⁵⁵. Las técnicas de seudonimización pueden tener carácter reversible (como las técnicas de criptografía simétrica o irreversible (aplicación de funciones *hash* en la criptografía asimétrica¹⁵⁶). Por lo tanto, de lo anterior se deduce que la seudonimización reversible seguirá perteneciendo a la categoría de "dato personal" y le será aplicable el nuevo Reglamento europeo, especialmente si su propósito es que más adelante pueda volver a reidentificarse a la persona física a quien afectan los datos. Mientras, la seudonimización irreversible podrá identificarse como información anónima, ya que la persona física dejará de ser identificable (Considerando 26 del RGPD).

Dado el escaso poder de negociación de los contratos de computación en la nube que ostenta el pequeño empresario, es de esperar que el proveedor sea quien elija el sistema que considere más óptimo para inutilizar los datos no útiles que ocupan espacio virtual en sus sistemas. Por tanto, en la práctica de los contratos de computación en la nube, bloquear, sobrescribir, destruir o anonimizar los datos personales será una elección del proveedor *cloud* como encargado del tratamiento, puesto que estas funciones forman parte de su deber de custodia de la información facilitada por el cliente pequeño empresario. Este, sin embargo, al ser quien suscribe los servicios *cloud* para tratar datos personales de terceros, es el responsable del

155 Dictamen 5/2014 del Grupo de Trabajo del Artículo 29, sobre técnicas de anonimización, pág. 22. [En línea], Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf>. [Fecha de consulta: 17 de febrero de 2017]

156 HON, W. Kuan; MILLARD, C; WALDEN, Ian, *What is Regulated as Personal Data...*, op. cit., pág. 171.

CAPÍTULO SÉPTIMO

tratamiento de esos datos (como se ha observado en capítulos anteriores) y, por ello, de la adecuada elección del proveedor *cloud* y del destino final de los datos personales. Consecuentemente, el pequeño empresario suscriptor, como responsable del tratamiento, debería estar en posición de dar instrucciones sobre estos extremos al proveedor *cloud* encargado del tratamiento.

Asimismo, debe tenerse en cuenta que, según la normativa de protección de datos, los procesos de anonimización, modificación, adaptación, supresión o destrucción de datos personales forman parte del abanico de operaciones que integran el tratamiento de datos personales¹⁵⁷.

Por último, cabe recordar al cliente empresario que no debe descuidarse, a pesar de lo anterior, de valorar adecuadamente el nivel de sensibilidad y criticidad de los datos que pretenda migrar a los sistemas del proveedor antes de proceder a la suscripción de cualesquiera servicios de computación en la nube, ya que en ocasiones, puede ser recomendable, para entender cumplido el deber de diligencia profesional que pueda serle exigible, un borrado seguro, riguroso y con las máximas garantías de verificación¹⁵⁸. Todo ello puede extraerse del artículo 32 del Reglamento General de Protección de Datos, dedicado a la seguridad del tratamiento¹⁵⁹.

157 Esto es así de acuerdo con la definición de "tratamiento" realizada por el artículo 4.2 del Reglamento 2016/679 ("cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción") y seudonimización del artículo 4.5 de la misma norma ("«seudonimización»: 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;" [recordemos que el concepto recogido por el Reglamento General de seudonimización engloba, a nuestro parecer, las técnicas que el Grupo de Trabajo del Artículo 29 define como seudonimización y como anonimización]). Aunque previa a estos conceptos, recogemos la vigente definición de "tratamiento" efectuada por el artículo 5.1.t) del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal ("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").

158 Para ciertas categorías de datos, consideramos más adecuado, como se ha dicho en el capítulo preliminar, otras alternativas a la implementación pública, como la adopción de entornos de nube privados, comunitarios o híbridos.

159 Art. 32.1 Reglamento General de Protección de Datos: "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

CAPÍTULO SÉPTIMO

Así, el diseño adecuado de mecanismos que permitan asegurar la privacidad de los titulares de datos personales es lo que viene entendiéndose en la industria como *Privacy by Design*, concepto que alcanzaría la decisión sobre el destino de esos datos una vez haya finalizado la relación entre proveedor y cliente *cloud* (anonimización, sobreescritura, etc.)¹⁶⁰. El artículo 25 del Reglamento General de Protección de Datos regula esta idea bajo el título "Protección de datos desde el diseño y por defecto", a través de diferentes obligaciones para el responsable. Así, establece que el responsable, cuando lo permitan el estado de la técnica, el coste de la aplicación y el fin del tratamiento, entre otros aspectos, deberá seleccionar adecuadamente los medios que utiliza para el tratamiento de los datos y minimizar la cantidad de datos personales que se tratarán, así como la duración de su tratamiento y periodo de conservación, e implementar medidas de cifrado (u otras similares) para impedir que estos datos sean accesibles por un número indeterminado de personas¹⁶¹.

En su aplicación en entornos de computación en la nube contratados por pequeños empresarios, este artículo obliga al empresario-responsable a tres acciones:

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 proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. (...)"

160 NOUGRÈRES, Ana Brian, "La protección inteligente de los datos personales: Privacy by Design", *Revista Internacional de Protección de Datos Personales*, Universidad de los Andes, Colombia, núm. 1, 2012. <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf>. [Fecha de consulta: 25 de mayo de 2016].

161 Artículo 25 del Reglamento 2016/679: "Protección de datos desde el diseño y por defecto. 1. 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. 2. 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. 3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo".

CAPÍTULO SÉPTIMO

la primera, seleccionar un adecuado mecanismo de implementación que le permita proceder al tratamiento de datos automatizado en la nube (nube pública, privada, etc.) y un proveedor *cloud* que le ofrezca suficientes garantías y confiabilidad como encargado del tratamiento. La segunda, a migrar únicamente los datos personales de terceros que resulten imprescindibles para el tratamiento y los fines que se persiguen. Y, por último, y puesto en relación con el artículo 32 del mismo Reglamento General, asegurarse de que se integran en el tratamiento medidas técnicas y organizativas que garanticen un nivel de seguridad adecuado al riesgo, lo cual puede incluir medidas como el cifrado o la seudonimización de los datos personales¹⁶². El alcance de estas obligaciones se ponderará, como hemos mencionado, de acuerdo con diferentes factores, como el coste de las aplicaciones, la naturaleza del tratamiento y los datos involucrados, etc.

Para demostrar el cumplimiento de estas obligaciones, el Reglamento promueve la adopción de certificaciones y sellos de garantía en materia de protección de datos, tal y como establece el artículo 42¹⁶³.

En resumen, la relevancia jurídica de la eliminación de los datos de los sistemas *cloud* consiste en que los derechos del cliente y de terceros queden

162 Art. 32 del Reglamento General de Protección de Datos. "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 proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento".

163 Art. 42 del Reglamento General de Protección de Datos. "Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas. 2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados(...)".

CAPÍTULO SÉPTIMO

salvaguardados, y ello puede compatibilizarse con copias de esos contenidos que se mantengan íntegras y confidenciales. Por otro lado, si esos datos tienen carácter personal, con un eficaz y robusto sistema de anonimización pueden utilizarse esos datos sin que se afecte a la privacidad de los interesados.

En nuestra opinión, el legislador ha intervenido adecuadamente, al incentivar el uso de las técnicas de anonimización y seudonimización¹⁶⁴ por parte de responsables y encargados del tratamiento de datos personales, y de cualesquiera otros mecanismos que minimicen las posibilidades de acceder a información digital comprensible, ya que aumentan el nivel de protección de los interesados y, en cuanto afecta a la privacidad, al dificultar la comisión de injerencias ilegítimas en la esfera de intimidad de los individuos¹⁶⁵. Estas medidas protegen los datos que se migran y se deben conservar en sistemas de computación en la nube ofreciendo mayores garantías que un almacenamiento simple.

Sin embargo, no debemos olvidar que en muchas ocasiones recae sobre la figura del cliente pequeño empresario, como responsable del tratamiento, la obligación de evaluar la viabilidad de estos mecanismos y adoptar de otras garantías complementarias que puedan resultar adecuadas respecto de los datos que trata (arts. 32 y 35 del Reglamento)¹⁶⁶. Por ello, opinamos que hubiera sido acertada alguna previsión que exigiera del proveedor *cloud* una máxima colaboración en estos procesos y la información a su cliente respecto de los mismos, especialmente en aquellos casos en los que el pequeño empresario puede desconocer la existencia de mecanismos de seudonimización que podrían aplicarse sobre los datos que trata, y las consecuencias legales de la no adopción de estos mecanismos minimizadores de riesgos.

164 Seguimos utilizando, en este caso, los conceptos recogidos por el Dictamen 5/2014 sobre técnicas de anonimización (WP216) elaborado por el Grupo de Trabajo del Artículo 29.

165 Por ejemplo, de sistemas de encriptado de información, fragmentaciones de datos, etc.

166 Artículo 35 del Reglamento europeo: "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; (...)".

CAPÍTULO SÉPTIMO

6.2.3.- La prueba del borrado de datos

La cuestión de la prueba de que, efectivamente, los datos migrados han sido adecuadamente tratados y eliminados del sistema *cloud* es muy importante para pequeños y medianos empresarios, especialmente en aquellos casos en los que los contenidos incluyan datos personales de terceros no anonimizados, o contengan información crítica sobre la empresa.

La eliminación de los datos resulta, en última instancia, un aspecto esencial en relación a la seguridad de los datos migrados, tengan o no carácter personal, puesto que un borrado ineficaz o inexistente puede provocar riesgos e incertezas en cuanto a su confidencialidad e integridad. Por contrapartida, un buen acuerdo de confidencialidad puede minimizar los riesgos de un mal proceso de borrado, aunque este tipo de acuerdo no sea frecuente en suscripciones de servicios de nube pública bajo condiciones generales de contratación.

Una opción para la obtención de un mecanismo de prueba podría ser la emisión, por el propio proveedor, de un certificado que acredite que efectivamente se han sometido los datos del cliente a un proceso de borrado que bloquee el acceso a tales archivos que serán sobrescritos gradualmente. El problema de esta medida es evidente: sin un tercero que acredite la veracidad de tal afirmación, el cliente debe confiar en lo afirmado por el proveedor, ya que difícilmente podrá comprobar, por sí mismo, la efectiva implementación de tal proceso y la eficacia del borrado, ya que únicamente podrá constatar que se han eliminado o se ha bloqueado el acceso a esos contenidos desde su cuenta de cliente.

Considerando la existencia de grandes riesgos para el pequeño empresario responsable del tratamiento de datos personales, el Reglamento General de Protección de Datos insta a las instituciones europeas, a los Estados miembros y a las autoridades en materia de protección de datos a adoptar mecanismos de certificación, los cuales ayudarían a incrementar la confianza entre proveedor de servicios *cloud* y cliente, y, en última instancia, entre responsable e interesado.

Para obtener estos sellos, el proveedor *cloud* deberá demostrar su cumplimiento en materia de protección de datos y la gestión de las instrucciones que el cliente de servicios pueda efectuar en su papel de responsable del tratamiento o de titular de tales datos. En nuestra opinión, esta resulta una iniciativa adecuada,

CAPÍTULO SÉPTIMO

novedosa respecto de la anterior Directiva y de nuestra Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, aunque habrá que observar con el tiempo si el uso de estos certificados llega a penetrar en el sector de computación en la nube, especialmente en relación a aquellos servicios gratuitos o de bajo coste.

6.3.- El borrado de datos como obligación del proveedor

Una vez expuestas las diferentes medidas relacionadas con el destino de los datos una vez finalizada la relación contractual entre el proveedor de servicios *cloud* y su cliente pequeño empresario, cabe plantearse si el borrado puede constituirse como una obligación esencial del proveedor de servicios *cloud*. Para responder a esta cuestión, debemos diferenciar entre las obligaciones del proveedor nacidas del contrato y aquellas obligaciones con otro origen, concretamente aquellas que emergen de la normativa en materia de protección de datos de carácter personal.

Respecto de las obligaciones que derivan de la naturaleza del contrato de computación en la nube, consideramos que debe entenderse incluido el derecho del cliente empresario, en la figura de suscriptor de un contrato de prestación de servicios (y no en su papel de responsable del tratamiento de datos de carácter personal), a conocer el destino de los datos remanentes en el sistema del proveedor una vez se ha extinguido el contrato. Ello es así porque la obligación de guarda y custodia ha expirado, con lo cual el proveedor debe procurar la máxima reversibilidad de los efectos del contrato sobre los datos titularidad del pequeño empresario, aunque sean datos de carácter no personal, sino fruto de la transmisión de información debido al uso ordinario del servicio *cloud*. Aplicando analógicamente la figura del depósito, por compartir con la computación en la nube la mencionada obligación de guarda y custodia, puesto que el depositario no puede servirse de lo depositado sin permiso expreso del depositante (art. 1767 del Código Civil¹⁶⁷) y ese permiso ha expirado a la vez que se extingue la relación contractual, es de entender que el proveedor no puede utilizar los datos migrados por el cliente ni de sus copias (según el art. 1770 del Código Civil, la cosa depositada será devuelta con todos sus

167 Art. 1767 del Código Civil: "El depositario no puede servirse de la cosa depositada sin permiso expreso del depositante. En caso contrario, responderá de los daños y perjuicios".

CAPÍTULO SÉPTIMO

productos y accesiones¹⁶⁸).

Por ello el proveedor *cloud* debe proceder a aplicar a los datos remanentes en sus sistemas ciertas medidas que garanticen al cliente suscriptor su bloqueo para que no serán utilizados en un futuro, así como intentar restaurar la situación en la cual tales réplicas de datos del cliente lleguen a desaparecer de los sistemas del proveedor. A nuestro parecer, es el proveedor quien, como profesional y de acuerdo con su deber de diligencia, debe instaurar, de acuerdo con las técnicas disponibles y con sus propias posibilidades, medidas técnicas que garanticen que los datos remanentes en sus sistemas que sean resultado de prestaciones ya extintas no puedan ser accedidos, utilizados o recuperados en un futuro.

Si el proveedor tiene datos procedentes de relaciones contractuales ya extintas almacenados en sus sistemas de manera segura, íntegra y confidencial, a la espera, por ejemplo, de que sean sobrescritos por otros datos para proceder a su borrado progresivo, en nuestra opinión el cliente no podrá exigir responsabilidades por el único motivo de que los datos no se hubieran eliminado en el momento de extinguirse el nexo jurídico, siempre y cuando la custodia de los datos se lleva a cabo en las condiciones de seguridad adecuadas y por motivos legítimos (por ejemplo, para evitar los elevados costes que supone la eliminación definitiva de esos datos). Ello es así porque, a nuestro parecer, el borrado de los datos no forma parte de las obligaciones principales de la naturaleza jurídica del contrato de computación en nube pública, a diferencia de lo que ocurre con el deber de custodia de esos datos. Recordemos que cuando los datos se someten varias veces a la sobrescritura, este borrado progresivo va dificultando su recuperación, pudiendo llegar a tener efectos sobre los datos asimilables al borrado definitivo, puesto que los datos se dejan igualmente de ser operativos y se imposibilita su reutilización o comprensión.

Dicho lo anterior, debemos enfatizar que, si se infringe la obligación de custodia de los datos que pudieron ser eliminados en el momento de extinguirse la relación jurídica y, por las razones que fueren, no se procedió a su borrado efectivo, el perjudicado podrá exigir una compensación por los daños causados (por ejemplo, si se vulnera su confidencialidad). En aquellos casos en los que el mismo contrato exonera al proveedor de cualquier responsabilidad por la infracción de este deber de

168 Art. 1770 del Código Civil: "La cosa depositada será devuelta con todos sus productos y accesiones. (...)".

CAPÍTULO SÉPTIMO

custodia post-contractual, deberá valorarse la validez de la cláusula que la contiene, es decir, si por su redacción es susceptible de calificarse como una cláusula abusiva o si puede contradecir a la propia naturaleza de la prestación y a la buena fe contractual¹⁶⁹.

Para finalizar la fundamentación de la obligación del proveedor de abstenerse de utilizar la información migrada por el cliente o facilitada por este durante el transcurso de la prestación, y junto con la extensión de la obligación de custodiar esa información mientras pueda ser inteligible, consideramos apropiado traer a colación la Propuesta de Directiva de suministro de contenidos digitales. En sus artículos 13.2.b) y 16.4.a), la Propuesta de Directiva establece la obligación para el proveedor, una vez el consumidor ha resuelto el contrato de suministro de contenidos digitales, o de abstenerse de utilizarlos o de ponerlos a disposición de terceros¹⁷⁰.

A primera vista, puede resultar sorprendente que estos mismos artículos no establezcan ninguna obligación para el proveedor de suministro de contenidos de custodiar esos datos remanentes o de transformarlos en ininteligibles para garantizar al consumidor que no se usen y que se mantienen confidenciales más allá de la extinción del contrato. Más aun cuando sí se le exigen estos extremos al consumidor respecto de los contenidos suministrados por el proveedor (arts. 13.2.d) y e) y 16.4.b) y c).

Esta falta de previsión se debe, en nuestra opinión, a la heterogeneidad de los contratos objeto de la norma. Estos diferentes contratos se integran bajo la denominación de "suministro de contenidos digitales", y, si bien la regulación incluye, como hemos mencionado, los servicios de computación en la nube suscritos por consumidores, no aborda de manera específica muchas de sus particularidades,

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

170 Propuesta de Directiva de suministro de contenidos digitales. Art. 13.2.b): "Cuando el consumidor resuelva el contrato: (...); b) el proveedor adoptará todas las medidas que podrían esperarse para abstenerse de utilizar las contraprestaciones no dinerarias que el consumidor haya facilitado a cambio de los contenidos digitales, así como cualesquiera otros datos recogidos por el proveedor en relación con el suministro de los contenidos digitales, incluido cualquier contenido facilitado por el consumidor a excepción del contenido que haya sido generado conjuntamente por el consumidor y otras personas que continúen haciendo uso del contenido". Art. 16.4.a): "Cuando el consumidor resuelva el contrato de conformidad con este artículo: a) el proveedor adoptará todas las medidas que podrían esperarse para abstenerse de utilizar contraprestaciones no dinerarias que el consumidor haya facilitado a cambio de los contenidos digitales, así como cualesquiera otros datos recogidos por el proveedor en relación con el suministro de los contenidos digitales, incluido cualquier contenido facilitado por el consumidor".

CAPÍTULO SÉPTIMO

siendo una de las más significativas la posibilidad de que, tras extinguirse el contrato, exista una cantidad ingente de datos (de carácter personal u otro tipo de datos) que, de quedar remanentes en los sistemas del proveedor, se ven abocados a una laguna sobre su destino y sobre las responsabilidades que puedan derivarse de su uso indebido o falta de confidencialidad.¹⁷¹

Estos artículos también refuerzan la idea de que el consumidor no puede exigir el borrado de los datos migrados al proveedor, sino que queda a discreción del proveedor su destino, siempre y cuando se abstenga de utilizarlos para sus propios fines. Como hemos mencionado en apartados anteriores, el hecho de que el borrado de los datos no sea exigible como una obligación principal del proveedor no obsta para que siga existiendo un deber de custodia de esos contenidos por parte del proveedor, aunque el contrato no esté vigente, debido a las propias particularidades de la prestación de servicios de computación en la nube.

En cuanto a las obligaciones derivadas de la normativa sobre privacidad y respecto de los datos que contengan información de carácter personal, cabe destacar que, en su papel de encargado del tratamiento, el proveedor de servicios de computación en la nube está obligado cumplir con lo exigido en el acuerdo con el cliente pequeño empresario (responsable del tratamiento) en cuanto al destino de esos datos, una vez su tratamiento deje de ser necesario, y en todo aquello que al respecto le exija la normativa sobre privacidad. En caso contrario, el proveedor deberá someterse al régimen sancionador establecido por la normativa aplicable, y puede ser considerado responsable del tratamiento a tales efectos, en cuanto infrinja

171 Propuesta de Directiva de suministro de contenidos digitales. Art. 13.2. d) y e) : "Cuando el consumidor resuelva el contrato: (...): d) si los datos digitales no se hubieran suministrado en un soporte duradero, el consumidor se abstendrá de utilizar los contenidos digitales o de ponerlos a disposición de terceros, en particular eliminando los contenidos digitales o transformándolos en ininteligibles, e) si los contenidos digitales se hubieran suministrado en un soporte duradero, el consumidor: i) a solicitud del proveedor devolverá, a expensas del proveedor, el soporte duradero a este último sin demora injustificada, y en cualquier caso no más tarde de 14 días desde la recepción de la solicitud del proveedor, y ii) eliminará cualquier copia utilizable de los contenidos digitales, los transformará en ininteligibles o se abstendrá de otra forma de utilizarlos o de ponerlos a disposición de terceros". Art. 16.4. b) y c) "Cuando el consumidor resuelva el contrato de conformidad con este artículo: (...) el proveedor facilitará al consumidor los medios técnicos para recuperar todos los contenidos facilitados por el consumidor, así como cualquier otro dato producido o generado mediante el uso por el consumidor de los contenidos digitales, en la medida en que estos haya sido retenidos por el proveedor. El consumidor tendrá derecho a recuperar los contenidos sin cargo alguno, sin mayores inconvenientes, en un plazo de tiempo razonable y con un formato de datos utilizado habitualmente, y c) cuando proceda, el consumidor eliminará cualquier copia utilizable de los contenidos digitales, los transformará en ininteligibles o se abstendrá de utilizarlos de otra forma, incluida la puesta a disposición de terceros".

CAPÍTULO SÉPTIMO

las obligaciones que le corresponden como encargado e incumpla las instrucciones del responsable, y ello afecte a la seguridad de los datos personales migrados por el cliente pequeño empresario que queden remanentes en sus sistemas.

En caso de vulnerarse la confidencialidad de esos datos custodiados, el titular de tales datos que se haya podido ver afectado tiene derecho a obtener una compensación por tal vulneración. Esta facultad aparece mucho más detallada y completa en la redacción del Reglamento General de Protección de Datos que en la Directiva 95/46/CE o en nuestra Ley Orgánica de Protección de Datos de Carácter Personal¹⁷². A efectos de conocer contra quién deberá interponerse la reclamación en cada caso, recordemos que la figura del responsable corresponderá generalmente al pequeño empresario que contrató servicios en la nube para tratar esos datos, aunque si el contrato lo suscribió el particular titular de los datos, directamente con el proveedor en la nube, el proveedor *cloud* será quien juegue el papel de responsable.

En resumen, la obligación de eliminar de manera definitiva los datos del cliente de los sistemas del proveedor, si bien puede suponer una obligación como cumplimiento de la normativa legal en materia de privacidad, no es exigible al proveedor como obligación principal derivada de la naturaleza del contrato de computación en la nube, ya que este puede conservarlos por diferentes motivos,

172 El derecho de indemnización de los interesados perjudicados aparece recogido en el artículo 19 de la Ley Orgánica en materia de Protección de Datos ("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. (...) 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria"), que transpone el artículo 23 de la Directiva 95/46/CE ("1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. 2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño"); y en el artículo 82 del Reglamento 2016/679 General de Protección de Datos: ("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. 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. 3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios. (..."). Ver apartado "Los efectos de finalización del contrato de computación en la nube sobre los datos personales", en el capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

CAPÍTULO SÉPTIMO

siendo uno de ellos la espera hasta que sean sobreescritos sucesivamente hasta que resulten prácticamente irrecuperables. Sin embargo, ello no impedirá que, ante problemas relacionados con la confidencialidad de estos datos, el proveedor de servicios deba responder incluso tras darse por extinguida la relación contractual entre las partes, como una extensión temporal del deber de custodia, el cual sí forma parte del contenido esencial del contrato de computación en la nube; ni tampoco impedirá que, en caso de vulnerarse la normativa de privacidad, el proveedor *cloud* deba indemnizar a los titulares de datos de carácter personal.

Por último, es conveniente recordar que la supresión de los datos personales de los sistemas del proveedor una vez finalizado el tratamiento es exigible por el titular de los datos, al ser uno de los derechos del interesado que le reconoce la normativa sobre privacidad respecto del control de su información personal. La Directiva 95/46/CE, nuestra Ley Orgánica de Protección de Datos y el recientemente aprobado Reglamento 2016/679 General de Protección de Datos reconocen al titular esta posibilidad, a través del ejercicio del derecho de cancelación (recogido en las dos primeras normas) o supresión (respecto de la regulación del Reglamento 2016/679). El nuevo Reglamento, además, regula como novedad el llamado "derecho al olvido"¹⁷³, respecto a la supresión de publicaciones en metabuscadores y en enlaces de datos relacionados con la intimidad de los particulares. En cuanto a las cuestiones relacionadas con el borrado de datos en la normativa de privacidad, y más concretamente con el derecho de cancelación, el derecho de supresión y el derecho al olvido, nos remitimos al capítulo sobre privacidad de este mismo trabajo.

173 Este derecho tiene origen en un caso judicial presentado ante tribunales españoles, en el marco del llamado "Caso Costeja", y que llegó hasta el Tribunal de Justicia de la Unión Europea. El Tribunal de Justicia de la Unión Europea sentenció, en 13 de mayo de 2014 (C-131/12), que el tratamiento que realizan los motores de búsqueda se somete a la normativa de privacidad europea y que los particulares tienen derecho a solicitar que sus datos personales, en ciertos casos, no figuren en los resultados de una búsqueda en Internet.

LA CONTRATACIÓN DE SERVICIOS DE COMPUTACIÓN EN LA NUBE POR EL PEQUEÑO EMPRESARIO TURÍSTICO

1.- INTRODUCCIÓN

En el capítulo inicial de este trabajo hemos enunciado las diferentes ventajas que brinda la tecnología de la computación en la nube, entre las que destacan el ahorro de costes en inversión, mantenimiento, actualizaciones y mejoras de la infraestructura informática; el acceso flexible e inmediato *online* a las capacidades que el cliente realmente demanda; su fiabilidad; la innecesariedad de elevados conocimientos técnicos o la facilidad para compartir y actualizar contenidos, aplicaciones y demás recursos computacionales tanto dentro de la propia organización como con terceros.

La industria del turismo no es ajena a las mejoras que ha proporcionado la tecnología de la computación en la nube, y con la adopción de estos servicios se beneficia de sus ventajas¹. Se estima que la computación en la nube puede suponer

1 Esta investigación se ha elaborado gracias al disfrute de la ayuda para formación de personal investigador predoctoral concedida por la *Conselleria d'Innovació, Recerca i Turisme* del Gobierno de las Islas Baleares y del Fondo Social Europeo, en el marco del Programa Operativo FSE 2014-2020. Igualmente, el presente trabajo se ha realizado en el marco de los Proyectos "Turismo y nuevas tecnologías; en especial, el régimen jurídico de las denominadas centrales electrónicas de reservas turísticas" (DER2012-32063), y "*Big data, Cloud Computing* y otros nuevos retos jurídicos planteados por las tecnologías emergentes; en particular, su incidencia en el sector turístico" (DER2015-63595), ambos bajo la dirección de la Catedrática Apol·lònia Martínez

CAPÍTULO OCTAVO

para las empresas turísticas un ahorro de costes que puede alcanzar el 40% en equipamiento informático, en comparación a las soluciones tradicionales². Además de reducir los gastos de adquisición y mantenimiento de equipos hardware y de actualización o renovación de software, la flexibilidad y escalabilidad que aporta la computación en la nube permite la adaptación del suministro a las concretas necesidades de la empresa turística, derivadas de aspectos como la estacionalidad o los picos de demanda propios de la actividad turística.

Según recientes informes, el 20,5% de las PYME y grandes empresas del sector que integra hoteles, campings y agencias de viajes declaran haber comprado algún tipo de servicio de *Cloud Computing* en el año 2015, así como el 6,9% de las microempresas que realizan estas mismas actividades empresariales³.

Asimismo, se observa una tendencia al alza respecto del uso y la contratación de servicios de computación en la nube, puesto que se ha producido un incremento respecto del año anterior tanto en las empresas de más de 10 trabajadores (5,5 puntos

Nadal como investigadora principal, financiados por la Dirección General de Investigación, del Ministerio de Economía y Competitividad y desarrollados en la Universitat de les Illes Balears. De ahí la inclusión de este capítulo específico referente al pequeño empresario del sector turístico como contratante de servicios de computación en la nube, sin perjuicio que los contenidos de los capítulos anteriores, predicables de la generalidad de contratos de computación en la nube pública suscritos por pequeños empresarios, puedan ser igualmente de aplicación.

- 2 Informe de las conclusiones del encuentro sectorial *Think Tank. Cloud Computing y Turismo*, impulsado por el Foro *Turismo.as* y la Sociedad Estatal para la Gestión de la Innovación y las Tecnologías Turísticas (SEGITTUR), celebrado en septiembre de 2012. Disponible en: <<http://www.segittur.es/opencms/export/sites/segitur/.content/galerias/descargas/notas-prensa/Informe-conclusiones-Think-Tank-Cloud-Computing-y-Turismo.pdf>>. [Fecha de consulta: 27 de febrero de 2017].
- 3 Estos datos se extraen del *Informe e-Pyme 2015*, elaborado por el Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información, que realiza un análisis sectorial de la implantación de las TIC en empresas españolas. Si bien hemos destacado los datos aportados por el mismo informe respecto del sector de hoteles, campings y agencias de viaje (integrado por 36.048 empresas de diferentes tamaños), cabe decir que en el mencionado informe se analizan también de manera diferenciada los sectores del transporte (terrestre, marítimo y aéreo) y del comercio minorista (el cual incluiría servicios de restauración y otros servicios turísticos de oferta complementaria). Este informe agrupa, por una parte, los datos de empresas de 10 o más trabajadores (PYME y grandes empresas) y, por otra, los datos de las microempresas (menos de 10 trabajadores) de los diferentes sectores empresariales. Estas últimas, según los datos aportados por Instituto Nacional de Estadística, integran el 95,8% del tejido empresarial español actual. Informe e-Pyme 2016 [en línea]. Disponible en: <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: 27 de febrero de 2017]

CAPÍTULO OCTAVO

más que en 2014) como en el caso de las microempresas (del 5,4% en 2014 al 6,9% en 2015) del mencionado sector. En el contexto actual, sin embargo, aún existen pequeños empresarios del sector turístico que desconocen la tecnología y la terminología referente al *Cloud Computing*, aunque en realidad sean, sin tener consciencia de ello, usuarios de algunos de estos servicios (como el correo electrónico, las redes sociales o el almacenamiento remoto de datos)⁴.

El correo electrónico, el almacenamiento de ficheros y las bases de datos en la nube, así como las redes sociales, se revelan como los servicios de *Cloud Computing* más adquiridos por las compañías del sector (hotelero, camping y agencias de viajes), independientemente de su tamaño. La implementación de otros servicios *cloud* es diferente según el tamaño de la empresa, destacando, en las microempresas, la implementación de aplicaciones *cloud* financieras o contables, las aplicaciones de software para tratar información sobre clientes o las suites ofimáticas⁵. Asimismo, se observa una tendencia creciente en la implementación de los servicios *cloud* en la pequeña y mediana empresa turística⁶.

Si bien la empresa turística aparece como una candidata ideal para utilizar estos servicios, permitiendo una mayor eficiencia y competitividad, también los turistas se benefician de las ventajas del *Cloud Computing*, puesto que muchos servicios en la nube están dedicados a optimizar la experiencia con el turista, y facilitar la interacción y el intercambio de información entre la comunidad de viajeros y entre el empresario turístico y los usuarios de sus servicios. Asimismo, el

4 PALOS SÁNCHEZ, Pedro R., AGUAYO CAMACHO, Mariano, *Los ecosistemas de Turismo Inteligente basados en Cloud Computing*, *El Turismo y la experiencia del cliente, Actas de las IX Jornadas de Investigación en Turismo*, Tomo II, Universidad de Sevilla, 2016, pág. 141. Respecto del concepto de computación en la nube y a la inclusión en su definición de servicios de correo electrónico o de redes sociales, nos remitimos al capítulo "Concepto y características técnicas de la computación en la nube".

5 Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información ONTSI, *Informe e-Pyme 2016* [en línea], 2016, pág. 122 Disponible en: <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: 27 de febrero de 2017].

6 Puede observarse esta tendencia creciente a partir de los informes "e-Pyme" elaborados por el ONTSI referentes a años anteriores. Informe año 2014, disponible en: <<http://www.ipyme.org/Publicaciones/informe-epyme-2014.pdf>>; informe año 2013, disponible en: <<http://www.red.es/redes/sala-de-prensa/convocatorias/presentacion-del-%E2%80%98informe-epyme-2013-analisis-sectorial-de-implantacion>>. [Fecha de consulta: 27 de febrero de 2017]

CAPÍTULO OCTAVO

pequeño empresario turístico puede valerse de la amplia oferta de software como servicio *cloud* (por ejemplo, aplicaciones informáticas) y de múltiples plataformas Web 2.0 (comparadores e intermediarios en la distribución de servicios turísticos) para valorar la percepción que tienen los clientes sobre la calidad de su prestación y aprovechar estas herramientas para tomar decisiones operativas de acuerdo con la información captada, optimizar la reputación empresarial, promocionar sus servicios, captar nuevos clientes y fidelizar a los ya existentes.

Pero los empresarios turísticos usuarios de la computación en la nube y de plataformas Web 2.0 también deben lidiar con los riesgos que esta revolución tecnológica implica. Respecto de la computación en la nube, existen riesgos que no pueden subestimarse, tales como la dependencia del proveedor y de la continuidad en la prestación del servicio, el cumplimiento de la normativa sobre privacidad o las cláusulas predispuestas y no negociables que provoquen un desequilibrio injustificado entre las partes. Por ello, y porque muchos de los servicios *cloud* contratados no son específicos para su sector, sino que están orientados para su contratación por cualquier usuario profesional, les serán de utilidad los aspectos generales de la contratación en la nube analizados en capítulos precedentes de este trabajo.

En este capítulo, especialmente dedicado a las relaciones jurídicas entre computación en la nube y pequeño empresario turístico, vamos a exponer, en primer lugar, una breve referencia a los servicios de computación en la nube más utilizados por el pequeño empresario turístico, ya sean de uso genérico o especialmente destinados a solucionar las necesidades técnicas de este sector. A continuación, realizaremos un análisis de la problemática jurídica que se deriva del uso de estos servicios, tanto desde una perspectiva contractual como desde la perspectiva de la normativa sobre privacidad. Por último, y dada la creciente expansión de las plataformas Web 2.0, hemos considerado oportuno mencionar algunas características contractuales comunes con la contratación de servicios *cloud*, así como diferentes problemáticas específicas a la relación entre estos operadores, el pequeño empresario turístico y la comunidad de viajeros.

2.- LA UTILIDAD DEL *CLOUD COMPUTING* EN EL SECTOR TURÍSTICO

Generalmente, las diferentes empresas dedicadas al sector turístico, ya sean empresas dedicadas al transporte, al alojamiento, a la restauración, a la intermediación, a la promoción turística o al ocio, tendrán a su disposición diferentes programas informáticos para gestionar de manera automática múltiples tareas relacionadas con su operativa empresarial.

Las distintas soluciones informáticas empresariales (ERP, CRM, suites ofimáticas, etc.) pueden estar alojadas en un servidor de la empresa cliente (físico o virtual), o basadas en computación en la nube, a modo de software como servicio (SaaS). Estas últimas suponen ventajas respecto de las primeras (soluciones tradicionales u *on premise*), entre las que destacan su sencillez de uso, la facilidad de implementación, la actualización automática del software, la no necesidad de adquirir hardware, la escalabilidad y flexibilidad adaptable a los picos de demanda propios del sector turístico, o la posibilidad de interconectar y relacionar información de manera automática proveniente de diferentes usuarios (clientes o empleados) y de diferentes módulos del software (por ejemplo, relacionar la información que incluye el directorio de proveedores con la información sobre inventarios o facturación), entre otras⁷. Todas estas ventajas redundan en una mejora de la productividad, la eficiencia y la competitividad, y en una disminución de costes.

Existen, pues, múltiples softwares como servicio (SaaS) utilizados por la industria turística cuyas funciones se solapan y se complementan. Dependiendo del modelo, tipo de actividad, dimensiones y recursos disponibles del negocio serán más recomendables unas u otras opciones, teniendo que plantearse aspectos como la necesidad o no de personalización del software, los costes asociados, la cantidad de información a manejar o la facilidad de la implementación en la operativa empresarial del software elegido⁸. A continuación, explicaremos brevemente las

7 Cabe decir que algunas de estas ventajas pueden igualmente conseguirse con equipos propios de la empresa turística que se conecten mediante redes internas. Sin embargo, en estos casos las funcionalidades estarán limitadas por las capacidades informáticas que soporten estas redes propias o servidores internos, con lo cual no puede hablarse de aspectos propios del *cloud* como la escalabilidad o la flexibilidad.

8 Según algunos estudios, los servicios más utilizados por hoteles independientes son los software

CAPÍTULO OCTAVO

funcionalidades de algunas de las herramientas de software basadas en la computación en la nube más extendidas entre los pequeños empresarios del sector turístico. Cabe destacar que esta clasificación no pretende ser una lista cerrada, puesto que existen multitud de soluciones especializadas, sino un muestrario de las soluciones de *Cloud Computing* más populares entre las empresas del sector turístico.

2.1.- Almacenamiento remoto de archivos y copias de seguridad

Se trata de un servicio en el cual un proveedor ofrece, el almacenamiento de archivos del cliente en uno o múltiples servidores físicos o virtuales, replicados en uno o varios centros de procesamiento de datos. Tal capacidad de almacenamiento remoto presenta las características generales de los servicios de computación en la nube, como la escalabilidad, la facilidad de uso o la elasticidad. El cliente de estos servicios, por su parte, puede almacenar archivos sin consumir recursos de memoria de su propio equipo hardware, y es quien administra y gestiona los archivos almacenados, accediendo a ellos a través de una interfaz de usuario desde cualquier dispositivo con conexión a Internet⁹.

Junto al servicio de correo electrónico, los softwares como servicio (SaaS) de almacenamiento remoto de datos se han convertido en los más populares entre particulares y pequeñas empresas, como se ha visto en capítulos anteriores de este trabajo. Respecto de su implementación en empresas del sector turístico, cabe decir que se trata de un tipo de servicio adaptable a cualquier empresa turística independientemente de la orientación de su actividad (transporte, alojamiento, restauración, ocio, intermediación, publicidad, etc.). En otros casos, el empresario turístico preferirá otras soluciones más completas o especializadas, como los servicios de *Hosting* de sitios web en la nube, que pueden presentarse a modo de servicios de infraestructura (IaaS) o plataforma (PaaS) y que mejoran las capacidades de procesamiento y de respuesta ante altos picos de demanda.

como servicio (SaaS) que permiten almacenar ficheros y realizar copias de seguridad, las suites ofimáticas o distintos sistemas de planificación de recursos empresariales (ERP, PMS, CRM, etc.). PALOS SÁNCHEZ, *Los ecosistemas de turismo...*, op. cit., págs. 139, 140; ONTSI, *Informe e-Pyme 2016*, op. cit., pág. 122.

⁹ Definición propia.

CAPÍTULO OCTAVO

Los servicios de almacenamiento remoto pueden ofrecer espacio virtual ampliable según las necesidades del cliente y sujeto a diferentes tarifas o planes, e incluso pueden prestarse a cambio de contraprestaciones no monetarias (por ejemplo, el cliente deberá ceder cierta información de carácter personal o con interés comercial y/o soportar publicidad no solicitada)¹⁰. Los software como servicio de almacenamiento remoto pueden presentar diferentes funcionalidades dependiendo del propio servicio, como la sincronización de ficheros, la compartición de archivos entre usuarios, aplicaciones que permitan editar los archivos almacenados, la gestión de copias de seguridad y restauración de datos, el cifrado de información en almacenamiento y en tránsito, etc.¹¹

2.1.2.- Correo electrónico y *suites* ofimáticas en la nube

Como es sabido, el correo electrónico se ha convertido en un servicio cotidiano y prácticamente imprescindible como mecanismo de comunicación, adoptado de manera masiva por particulares, empresas de todo tipo y organizaciones públicas, gracias a su uso sencillo y al ahorro en costes en papel y en servicios de mensajería tradicional. Además, la posibilidad de obtenerlos de manera "gratuita" o con tarifas muy económicas es otro aliciente que particulares y pequeños empresarios valoran especialmente, entre ellos, el pequeño empresario turístico, sea cual sea su concreta actividad económica¹².

10 Para más información sobre las contraprestaciones no dinerarias, nos remitimos a ROSSELLÓ RUBERT, Francisca María, "Las contraprestaciones no dinerarias en la Propuesta de Directiva sobre suministro de contenidos digitales", Revista de Derecho Mercantil, núm. 303, 2017, págs. 163-190.

11 Algunos de los software como servicio (SaaS) de almacenamiento remoto más conocidos son *Dropbox*, *G-Suite* (antes *Google Drive*), *Amazon Cloud Drive*, *Apple iCloud*, *Box* o *Microsoft OneDrive*.

12 En 2007 algunos estudios revelaron que el correo electrónico era una de las herramientas básicas de comunicación entre establecimientos de turismo rural y clientes, siendo sus usos más frecuentes el envío de información sobre el establecimiento, el esclarecimiento de dudas y la confirmación de reservas. El mismo informe también ponía de relieve que el 84% de esta categoría de establecimientos utilizaba para la gestión interna herramientas de ofimática, aunque las aplicaciones destinadas al negocio hotelero estaban poco implementadas en esos momentos. OBSERVATORIO DE LAS TELECOMUNICACIONES Y LA SOCIEDAD DE LA INFORMACIÓN; ENTIDAD PÚBLICA EMPRESARIAL Red.es, *Informe Diagnóstico Tecnológico Turismo rural* [en línea], 2007, pág. 8. Disponible en: <<https://es.scribd.com/document/34878355/Diagnostico-tecnologico-Turismo-rural-2007>>. [Fecha de consulta: 8 de marzo de 2017].

CAPÍTULO OCTAVO

Tradicionalmente, el servicio de correo electrónico se prestaba mediante sistemas de arquitectura cliente-servidor o se alojaban en equipos locales de la propia organización. La implementación en la nube de este servicio le convierte en uno de los softwares como servicio (SaaS) más utilizados, permitiendo a los usuarios crear, almacenar, enviar y recibir mensajes electrónicos y archivos digitales a través de Internet sin tener que utilizar recursos hardware del cliente, así como otras funciones adicionales que optimizan su rendimiento, como filtros *antispam* (contra la entrada masiva de mensajes) o antivirus, o sincronizaciones con otros servicios (como agenda, calendario o listas de contactos)¹³. Pueden comercializarse como un servicio independiente o como parte de un conjunto de aplicaciones integradas dentro de las denominadas suites ofimáticas¹⁴.

Las suites ofimáticas, también conocidas como "oficina virtual", integran un conjunto de aplicaciones informáticas mayormente utilizadas en actividades administrativas y de oficina, como procesadores de texto y hojas de cálculo, programas para elaborar presentaciones, gestores de bases de datos, correo electrónico, agenda personal, bloc de notas, calendario, etc. Si bien tradicionalmente se ejecutaban a través de la instalación de software en el equipo informático del cliente, la opción ofimática basada en tecnología *cloud* se ejecuta a través de una plataforma web y los datos se almacenan en servidores remotos, con lo cual no es necesario descargar la suite completa¹⁵ en el equipo físico del cliente, y así no consume recursos propios, sino los suministrados por el proveedor *cloud*¹⁶.

Este conjunto de aplicaciones tienen como funcionalidades crear, editar, almacenar o compartir archivos y documentos. Al estar orientadas a entornos profesionales, generalmente las suites de ofimática en la nube se ofertan a cambio de precio, si bien pueden encontrarse en el mercado opciones "gratuitas" con funcionalidades limitadas¹⁷. Asimismo, como las tareas que pueden gestionarse a

13 Definición propia.

14 Algunos de los software como servicio de correo electrónico más conocidos son *Google Gmail*, *Amazon Simple Email Service*, *Microsoft Outlook* o *Yahoo Mail*.

15 Sucede en algunos servicios de ofimática que no se despliegan totalmente sobre la plataforma *cloud*, con lo cual es necesario instalar parte de la *suite* en el equipo *hardware* del cliente, como sucede con *Microsoft Office 365*.

16 Definición propia.

17 Entre los servicios *cloud* de *suite* ofimática más destacados, pueden mencionarse *Google G-Suite* (antes *Google Apps for Work*), *Zoho Workplace*, *Apple iWork* o *Microsoft Office 365*. A modo de ejemplo de suite ofimática gratuita, *Microsoft Office Online*.

CAPÍTULO OCTAVO

través de una suite ofimática son comunes para la amplia generalidad de actividades empresariales, son susceptibles de utilizarse por empresas turísticas de cualquier rama (alojamiento, transporte, intermediación, ocio, etc.).

2.3.- Sistemas de gestión de recursos empresariales (*Enterprise Resource Planning* o ERP)

Este software tiene como finalidad el manejo de información sobre los diferentes recursos empresariales, y para ello facilita la gestión de la actividad empresarial en aspectos operativos tales como contabilidad y facturación, ventas, disponibilidad de plazas, inventarios, recursos humanos, proyectos, adquisiciones, contratación, etc. Así, su principal utilidad es la integración en un único sistema del máximo número de procesos corporativos¹⁸. La integración de toda la información sobre los recursos empresariales, manejada mediante sistemas *Enterprise Resource Planning* (también conocidos por las siglas ERP), ayuda a tener un mayor control y mejorar la planificación sobre los activos, a prever los beneficios y costes operacionales, a mejorar de la productividad, y a una mejor toma de decisiones.

Esta información se suele reservar al funcionamiento empresarial, únicamente se accede a ella por parte de componentes o socios de la entidad, entre quienes puede compartirse, y no resulta accesible para los clientes o el público en general. Gracias a los sistemas en la nube, además, está información puede ser accesible desde los diferentes dispositivos con conexión a Internet de los usuarios autorizados, quienes dispondrán de la información actualizada prácticamente en tiempo real.

Las soluciones ERP pueden presentarse en un formato genérico, ampliamente flexible, configurable y adaptable a las necesidades de cualesquiera empresas de similares tamaños y necesidades, o en formatos especialmente orientados a ciertas actividades empresariales, atendiendo a las específicas exigencias y problemáticas operativas de un determinado sector o industria, como el turístico¹⁹. Aunque tradicionalmente se prestaban mediante arquitectura cliente-servidor, en la

¹⁸ Definición propia.

¹⁹ Como ejemplo de formato genérico de Software como Servicio de ERP para pequeñas empresas, podemos citar *Oracle Enterprise Resource Planning*, *Microsoft Dynamics NAV*, u *Odoo*.

CAPÍTULO OCTAVO

actualidad muchos de estos sistemas se ofertan a modo de software como servicio (SaaS), permitiendo el ahorro de costes en infraestructura, la escalabilidad y el acceso a la información a través de Internet, entre otras ventajas anteriormente comentadas. Aunque existen soluciones "gratuitas", los sistemas ERP más completos son servicios de pago. También es habitual que se comercialicen de manera separada a través de módulos que permiten gestionar distintas áreas de negocio, pudiéndose combinar varios de ellos y sin necesidad de acceder al conjunto de prestaciones, con el consiguiente ahorro para el pequeño empresario.

Entre la categoría de sistemas ERP, cabe decir que van apareciendo en el mercado distintas soluciones de sistemas de gestión adaptadas a las concretas necesidades que presentan las diferentes actividades económicas del sector²⁰.

20 En primer lugar y centrando nuestra atención en el pequeño empresario turístico, podemos destacar los sistemas *Property Management System* (PMS) o sistemas operativos de gestión integral de servicios de alojamiento (establecimientos hoteleros, casas rurales, apartamentos vacacionales, hostales, campings, etc.). Son programas informáticos especialmente dedicados a automatizar los principales procesos para la prestación de estos servicios, cubriendo áreas específicas como las reservas de clientes *online* y *offline*, entradas y salidas de huéspedes (*check-in* y *check-out*), establecimiento de tarifas, gestión de cobros y facturas, administración del mantenimiento y del inventario del establecimiento, datáfono, sistemas de gestión de información de clientes, acciones comerciales, sistemas de gestión de ingresos (*Revenue Management Systems* o RMS), etc. Tienen como finalidad reunir en un único producto la mayoría de procesos operativos del establecimiento, interconectando la comercialización de reservas hoteleras con la gestión interna de recursos, mantenimiento y personal del establecimiento. (Definición propia. Como ejemplos de SaaS PMS "gratuitos", *Avirato* o *Bitte*, y como ejemplos de pago, *Micros* o *Protel*. Como hemos dicho, los sistemas centrales de reservas o CRS (*Central Reservation System*) generalmente forma parte integrante de un producto PMS, o puede vincularse a este, puesto que es esencial que la información del módulo de reservas y el de inventario del establecimiento pueda relacionarse y complementarse. Este software tiene como función principal gestionar las reservas realizadas, y permite ajustar el precio del producto a la disponibilidad prevista y ayuda a determinar el canal de comercialización más adecuado. Por otra parte, existen soluciones de gestión especializadas en establecimientos de restauración, que suelen ofertarse a través de sistemas modulares, y generalmente disponen de herramientas para administrar la ocupación y las reservas *online* y *offline* del establecimiento, sistemas de reconocimiento de llamadas entrantes de clientes, organización de la actividad del personal (distribución de tareas, mesas y turnos entre camareros, comunicación entre cocina, barra y servicio, etc.), configuración de cartas y menús, administración de cartera de clientes y envío de mensajes promocionales, interacción con terminales TPV y cajas registradoras, consulta de ventas y estadísticas, etc. Algunas soluciones especialmente diseñadas para restaurantes, bares, cafeterías y otros establecimientos de restauración son Engisoft POS Mobile (con una aplicación gratuita básica y una completa versión *premium* de pago), [*Siscovcloud* para restaurantes o *Marketman*. También existen ERP en la nube especialmente pensadas para agencias de viaje *online*, como *Conpas* o *Giav* de Gesintur.

2.4.- Sistemas de gestión de clientes (*Customer Relationship Management* o CRM)

La función principal de los sistemas software CRM es recoger de manera organizada la máxima información del cliente para que el empresario pueda adelantarse a sus necesidades, coordinándola con acciones de marketing. Para ello, puede disponer de diferentes funcionalidades, como la automatización de procesos de venta, bases de datos de clientes, administración de actividades relacionadas con la atención al cliente, gestión de redes sociales y *e-mailing*, etc²¹.

Si bien en ocasiones forman parte de un sistema integral de planificación de recursos empresariales o ERP, también es común que el módulo de gestión CRM se comercialice separadamente²².

2.5.- Sistemas de gestión de la reputación *online* (*Online Reputation Management* u ORM)

Los sistemas ORM o de gestión de la reputación son software como servicio (SaaS) que permiten monitorizar los comentarios y opiniones que la comunidad de usuarios ha vertido sobre un establecimiento o marca empresarial a través de distintos canales (redes sociales, agencias de intermediación, comparadores, blogs, foros, etc.) para así poder efectuar un control sobre la reputación *online* y gestionar la marca empresarial²³. Puede incorporar otras funcionalidades, como la monitorización de la posición del hotel en los principales buscadores o de las fotografías y vídeos publicados en Internet sobre el establecimiento o marca. Pueden ser utilizados para cualquier tipo de negocio turístico, aunque especialmente se

21 Definición propia.

22 Según han revelado recientes estudios, el 56,6% de las empresas españolas utiliza un software CRM, y de estas, el 50,49% tiene alojados sus sistemas CRM en la nube. Estudio "Las herramientas de marketing y ventas y el uso del CRM en las empresas españolas en 2016", elaborado por el comparador de soluciones empresariales SoftDoit. Disponible en: <<https://www.softwaredoit.es/estudio/estudio-herramientas-marketing-ventas-uso-software-crm-empresas-espana-2016.html>>. [Fecha de consulta: 6 de marzo de 2017]. Como ejemplos de servicios de gestión de clientes en la nube para pequeños empresarios, podemos destacar *Zoho Online CRM*, *Microsoft Dynamics CRM*, *ProsperWorks*, *Teamleader*, *Nube CRM* (el cual tiene un SaaS con funcionalidades básicas "gratis") o los "gratuitos" *Suma CRM* o *Karma CRM*.

23 Definición propia. Por ejemplo, *Rategain* o *ReviewPro*.

CAPÍTULO OCTAVO

recomiendan para establecimientos hoteleros y de restauración.

2.6.- Alojamiento de páginas web en la nube o *Cloud Hosting*

Con el alojamiento de sitios web (estáticos) o de aplicaciones web (sitios web dinámicos que incluyen funcionalidades como tiendas *online* o *blogs*) en la nube pública, el proveedor *cloud* dispone de una red integrada por múltiples servidores interconectados que garantizan la prestación al cliente con una mayor fiabilidad, puesto que es común que estén distribuidos entre distintos centros de datos geográficamente dispersos, en lugar de en uno solo, como sucede con el *Hosting* tradicional²⁴. Ofrecen al cliente capacidad de procesamiento, espacio en disco y memoria RAM, entre otras funcionalidades.

El *Hosting* en la nube puede presentarse al cliente a modo de infraestructura como servicio (IaaS), en la cual se le proporciona el hardware virtualizado, en el cual puede instalar diferentes entornos software (sistemas operativos, software para servidores web, herramientas de programación, etc.) y crear sobre él su propia aplicación web o alojar los contenidos de sus webs estáticas. Si se proporciona a modo de plataforma como servicio (PaaS), el cliente recibe un entorno software ya preinstalado y sobre el cual puede desarrollar y ejecutar sus aplicaciones y sitios web. El servicio de plataforma tiene un manejo más sencillo que el de infraestructura, aunque resulta menos personalizable.

Así, se consigue una mayor elasticidad, debido a la adecuación de los recursos que se necesitan de acuerdo con los picos de demanda en tiempo prácticamente real, como cuando se necesita una mayor capacidad para aguantar elevados volúmenes de tráfico de visitantes del sitio web o se pretenden implementar nuevas funcionalidades en la aplicación web. Del mismo modo, se permite al cliente escalar recursos de forma inmediata para poder atender a la demanda cambiante y ajustándose generalmente el precio a los recursos realmente consumidos, sin

24 En el 2007 ya se estimaba que cuatro de cada cinco empresas dedicadas al turismo rural (un 78,7%) disponían de página web. En su inmensa mayoría, estos establecimientos eran microempresas de menos de 10 trabajadores, y su uso de la página web se centraba principalmente en ofrecer información detallada sobre el destino y el establecimiento y la realización de reservas *online*. Observatorio de las Telecomunicaciones y la Sociedad de la Información; Entidad Pública Empresarial Red.es, *Informe Diagnóstico Tecnológico...*, op. cit., pág. 9.

CAPÍTULO OCTAVO

desperdiciar capacidades que se han contratado y no se utilizan cuando la demanda es más baja. En sistemas de *Hosting* tradicionales, la capacidad que puede obtener el cliente se ve limitada por la capacidad del servidor físico que aloja el sitio o aplicación web. Al ser diseñados para su uso sencillo y a modo de autoservicio, el cliente de servicios *Hosting* web en la nube tiene una mayor facilidad para gestionar los contenidos de su sitio web. Asimismo, al tratarse de sistemas redundantes, permiten prevenir o recuperarse de fallos de sistemas o componentes.

2.7.- Otros usos de la computación en la nube en el sector turístico

Si bien la anterior clasificación integra los principales servicios contratados por el pequeño empresario del sector turístico, existen otros muchos servicios implementados en la nube que pueden integrarse en la operativa empresarial de profesionales y empresarios del sector turístico, como los terminales punto de venta (TPV) en la nube (especialmente útiles para el sector de la restauración y servicios turísticos destinados al ocio)²⁵, los sistemas de gestión de ingresos (*Revenue Management Systems* o RMS)²⁶ u otras soluciones de inteligencia empresarial (*business intelligence*)²⁷, los sistemas de gestión de canales de distribución (*Channel Management System* o CMS)²⁸, etc.

25 Los TPV en la nube ofrecen funcionalidades añadidas a las que ofrece el TPV tradicional, como la conexión de múltiples y diversos periféricos (lectores de tarjetas, expendedores de bebidas, etc.). pagos mediante teléfonos móviles, la integración de la información de diferentes comercios o tiendas *online*, el control del stock disponible en tiempo real o la gestión de información de clientes y estadísticas de acuerdo con los datos obtenidos por los distintos terminales. Como ejemplos, *HioPos Cloud*, *iSelz* o *Axos Connect*.

26 Las soluciones de *Revenue Management Systems* suelen estar más orientados a establecimientos turísticos. Permiten predecir el comportamiento del consumidor a través de herramientas analíticas, mejorando la toma de decisiones de marketing. Con estas soluciones se facilita la tarea de ofertar el producto más adecuado a cada cliente, con una antelación adecuada y al precio adecuado según la ocupación del establecimiento, pudiendo controlar la administración y gestión de sus tarifas y la paridad de precios en los diferentes canales de distribución.

27 Son herramientas software destinadas a la recopilación y análisis de datos sobre el rendimiento de cualquier negocio, que permiten elaborar informes y estadísticas para poder proceder a una mejor toma de decisiones empresariales y de marketing.

28 Asimismo, existen programas informáticos para controlar la información facilitada por los sistemas de gestión de ingresos y coordinar múltiples canales de venta *online* de reservas, denominados CMS (*Channel Management Systems*) o Sistemas de Gestión de Canales. Se sincronizan sistemas de gestión integrales (ERP) y sistemas de agencias de viaje *online* (OTAs),

CAPÍTULO OCTAVO

Asimismo, el denominado *marketing* social, que supone la utilización de las redes sociales para la promoción de una empresa y la valoración de su imagen corporativa, resulta esencial en el sector del turismo y el ocio. Su uso está bastante extendido en microempresas del sector turístico, tal y como demuestran algunos estudios recientes²⁹. El pequeño empresario turístico que quiera promocionarse a través de estas plataformas deberá abrir una cuenta de usuario (o perfil) y sujetarse igualmente a las condiciones contractuales predisuestas por el proveedor de red social³⁰.

En resumen, la arquitectura de computación en la nube no solo ha permitido reducir costes en infraestructura informática, sino también expandir los servicios turísticos, personalizar la experiencia del cliente e integrar el uso de las tecnologías móviles para que empresa y turista interactúen. Las anteriores soluciones basadas en la computación en la nube y otras que se ofertan en el mercado digital actual permiten a la empresa turística aligerar la carga de trabajo relacionada con la infraestructura tecnológica y poder centrarse en su propia actividad empresarial³¹.

turoperadores u otros canales de distribución y permiten agilizar los procesos de envío de información de manera directa y en los diferentes canales permitiendo una gestión integral y automatizada de la oferta. Como ejemplo, los softwares como servicio (SaaS) *EZYield Hospitality Suite* o *Bookincenter*.

29 Un estudio de Telefónica, en colaboración con la entidad pública empresarial de Ministerio de Energía, Turismo y Agenda Digital *Red.es*, afirma que las microempresas del sector turístico se centran en la promoción de sus servicios y en la captación de clientes, aunque su utilización adolece de falta de planificación, profesionalización y medición de resultados. Las redes más utilizadas son Facebook, Twitter, FourSquare y Twenty. FUNDACIÓN TELEFÓNICA, "Desarrollo Empresarial y Redes Sociales. El caso de las microempresas españolas" [en línea], 2015, pág. 126. Disponible en: <http://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/331/>. [Fecha de consulta: 17 de marzo de 2017].

30 También conocido bajo otros nombres, como *e-marketing*, *marketing* digital o *geomarketing*, consigue un tipo de publicidad que interacciona directamente con el cliente, que genera resultados inmediatos, es flexible y puede segmentarse fácilmente según el público al cual pretenda orientarse. APARICIO VAQUERO, Juan Pablo, "Negocios y contratación en Internet. El ejemplo de los portales de ocio y viajes", en *FODERTICS, estudios sobre Derecho y Nuevas Tecnologías* (Coord. Federico Bueno de Mata), La Coruña, 2012, pág. 77.

31 Las empresas desarrolladoras de software especialmente orientado a soluciones informáticas para el sector turístico también suelen basar parte de su actividad empresarial en servicios *cloud* de infraestructura y plataforma para soportar cargas de procesamiento y almacenamiento, y utilizar herramientas de desarrollo y testeado. Por ejemplo, la *startup* desarrolladora de tecnología hotelera Hotel Ninjas sustentaba sus servicios en plataformas de Salesforce. Esta empresa fue adquirida en 2014 por el grupo Priceline, uno de los proveedores de viajes *online* líderes en el mercado con sitios web como *Booking* o *Kayak*. Ver noticias en

CAPÍTULO OCTAVO

Por último, cabe comentar que la arquitectura en la nube también sirve de soporte a plataformas web especialmente populares en el sector turístico, como los comparadores o las plataformas inteligentes de promoción de destinos, así como el análisis de datos o *Big Data* o el "Internet de las Cosas" (*Internet of things* o IoT). En posteriores apartados comentaremos brevemente algunos aspectos de las plataformas web 2.0 en el sector turístico.

3.- LA PROBLEMÁTICA JURÍDICA DEL *CLOUD COMPUTING* ESPECÍFICA DE SERVICIOS DESTINADOS AL SECTOR TURÍSTICO

En capítulos anteriores se han observado los principales problemas que presenta la contratación de servicios de computación en la nube, tales como que el cliente del servicio *cloud* no posee acceso directo a la información migrada al servidor remoto del proveedor, con lo cual se produce una pérdida de control sobre esos contenidos, su ubicación y las medidas de seguridad que se le aplican. Además, hemos estudiado varios problemas jurídicos que se hallan en muchos de los contratos predispuestos por los proveedores de estos servicios, como cuestiones de propiedad intelectual, determinación de la naturaleza jurídica del contrato o cláusulas desequilibradas que pueden privar al adherente del ejercicio de acciones y de la obtención de compensaciones por prestaciones deficientes.

Si nos centramos en los suscriptores de servicios de computación en la nube pertenecientes al sector turístico, nos encontramos con que algunos de estos problemas se acentúan debido a ciertas características de la actividad turística. Así, la estacionalidad de la prestación y los picos de demanda sugieren que eventuales problemas con la disponibilidad del servicio pueden ocasionar especiales pérdidas al pequeño empresario del sector turístico, quien, como sucede en la gran mayoría de ocasiones, no habrá tenido ocasión de negociar el contrato. A continuación, expondremos algunos de los problemas jurídicos detectados en contratos de servicios de computación en la nube que suelen suscribir profesionales de la actividad turística.

<<http://www.tecnohotelnews.com/2013/09/hotel-ninjas-se-alia-con-salesforce-para-ampliar-sus-servicios-en-la-nube/>> y <https://www.hosteltur.com/159150_priceline-compra-start-up-espanola-hotel-ninjas.html>. [Fecha de consulta: 13 de marzo de 2017].

3.1. El objeto del contrato predispuesto: ¿cesiones de licencia de software o servicios de computación en la nube?

Cualquier software que forme parte del servicio de computación en la nube que se presta al pequeño empresario es objeto de protección por parte de la normativa de propiedad intelectual. Por este motivo, es habitual que en los términos y condiciones que se suscriben al contratar el servicio *cloud* se concedan derechos para utilizar los programas informáticos involucrados en la prestación y facilitados por el proveedor *cloud*, sujetándolos a operaciones internas del negocio del empresario cliente³².

Generalmente, el contrato de computación en la nube contiene un apartado o conjunto de cláusulas en los cuales se concede una licencia de uso de la plataforma software al suscriptor del servicio; licencia que suele ser revocable, no exclusiva e intransferible, y puede retribuirse o no mediante un precio. Como resultado de esta concesión, el proveedor retiene la propiedad intelectual sobre los productos software, marcas, nombres comerciales, ingeniería y otros activos relacionados con la prestación del servicio, y se reserva los derechos no licenciados expresamente en el contrato. A su vez, el proveedor *cloud* permite al cliente suscriptor el uso de esos programas para una adecuada prestación de los servicios *cloud*, aunque ese uso está sujeto a ciertas restricciones y prohibiciones que variarán dependiendo del tipo de servicio *cloud* suscrito (no transformar ese software, comunicarlo públicamente, hacer copias no autorizadas, transferirlo, difundirlo, explotarlo comercialmente, etc.)³³.

Sin embargo, el pequeño empresario turístico debe tener en cuenta que los contratos de servicios de computación en la nube van más allá de una simple licencia de uso de software tradicional³⁴. Así, si en el formato *offline* el pequeño empresario disponía de una copia licenciada del software de gestión instalado en el sistema informático de la empresa, con la contratación de servicios de computación en la

32 Ver capítulo "Aspectos jurídicos de los contenidos alojados en la nube", en este mismo trabajo.

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

34 La mayoría de contratos de servicios utilizan diferentes descripciones para denominar a los contratos de software como servicio, por ejemplo "condiciones generales de uso" (como el proveedor Engisoft), "términos de servicios *online*" (Microsoft) o "contrato de alta del servicio y pago por uso de licencia" (Appinclusive).

CAPÍTULO OCTAVO

nube el almacenamiento de información y el procesamiento de datos tiene lugar en los sistemas del proveedor *cloud*, con lo cual existen otros aspectos de la prestación añadidos a la cesión de licencia tradicional que deben tenerse en cuenta. Se trata, por una parte, de obligaciones propias del proveedor de servicios de computación en la nube, como la continuidad en la prestación del servicio, la conservación de la información migrada en condiciones óptimas de seguridad o la recuperación y portabilidad de contenidos, que para mantener la operativa empresarial sin interrupciones pueden ser de suma importancia. Por otra parte, también comprenderá obligaciones para el cliente pequeño empresario turístico respecto del uso correcto y leal que debe realizar del servicio y de la responsabilidad por los contenidos de los archivos migrados, habitualmente contenidas en las políticas de uso adecuado (PUA).

Asimismo, puede que el cliente *cloud*, para poder utilizar el servicio, deba instalar determinado software del proveedor en su equipo o en varios dispositivos, por ejemplo, teléfonos móviles, sin que por ello se esté modificando el objeto contractual. Lo idóneo es el proveedor especifique de manera clara que se contrata, por una parte, el alta a un servicio de computación en la nube, y, al ser necesario para la prestación de este servicio el uso de software sujeto a derechos de propiedad intelectual, se acuerda también la concesión de una licencia de software, incluyéndose los términos de esta licencia en las condiciones y términos de uso del servicio *cloud*³⁵.

3.2.- Imposibilidad de negociación contractual

El pequeño empresario normalmente carece de oportunidad de negociación a la hora de suscribir contratos de computación en la nube. Independientemente de que los servicios *cloud* se oferten por grandes multinacionales o por pequeñas *start-ups*, al tratarse de servicios o aplicaciones pensadas para su comercialización en masa, el proveedor siempre es quien redacta las condiciones contractuales y las predispone para su suscripción a las empresas y profesionales interesados. En ellas intentará optimizar sus beneficios y, por norma general, trasladar el mayor número de riesgos

35 Ver "Obligaciones del proveedor", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

CAPÍTULO OCTAVO

al empresario suscriptor.

Por ello, el empresario suscriptor debe prestar atención al contenido contractual, como parte de su deber de diligencia profesional, especialmente si la continuidad de la actividad empresarial puede verse comprometida en el caso en que el servicio *cloud* se vea interrumpido o sea deficiente. Cuando la información facilitada por el proveedor no sea clara, precisa o completa respecto de los elementos integrantes del servicio, es recomendable ampliarla antes de contratar.

Asimismo, el pequeño empresario turístico suscriptor de servicios *cloud* deberá prestar especial atención a los aspectos sobre seguridad de la información migrada (pues esta información puede afectar a secretos empresariales o a otros activos del negocio), a las cláusulas de exención y limitación de responsabilidades y a las estipulaciones referentes a la finalización del contrato y sus efectos.

3.3.- Limitación y exclusión de responsabilidades

Los contratos de computación en la nube establecen en su clausulado la distribución de riesgos entre las partes ante deficiencias en la prestación. El proveedor no garantizará plenamente el funcionamiento del servicio, puesto que, al tratarse de un servicio fundamentado en tecnología informática compleja, existen múltiples factores que afectan al rendimiento y seguridad del sistema *cloud*. Por otra parte, es frecuente que el software implicado en la prestación carezca de un mecanismo de tolerancia a errores, con lo cual no estará libre de interrupciones o bloqueos.

Cada proveedor lidiará de manera diferente con los incidentes directamente relacionados con la calidad del servicio, y así lo establecerá en el clausulado contractual predispuesto para su suscripción por el pequeño empresario turístico. No es extraño encontrar en los contratos limitaciones y exoneraciones de responsabilidad que, si bien en algunos casos son comprensibles, al tratarse de riesgos que escapan del control del proveedor (ataques maliciosos, sobrecargas de Internet, etc.), en otras ocasiones la validez de estas cláusulas puede ser más discutible, en cuanto concierna a incumplimientos ocasionados por la falta de diligencia

CAPÍTULO OCTAVO

profesional del prestador de servicios³⁶.

De este modo, es habitual encontrarse en los contratos de computación en la nube con cláusulas que establecen una serie de exoneraciones y limitaciones de responsabilidad más o menos amplias, no garantizando que el servicio esté operativo la totalidad del tiempo, que no sea vulnerable a errores, interferencias o averías. Existen proveedores que optan por excluir cualquier responsabilidad derivada del servicio, por motivos de calidad, disponibilidad, continuidad, defectos u otros factores, en la medida en que la ley aplicable al contrato lo permita, incluso aunque el proveedor cause esas anomalía directamente, a través de una acción u omisión, o aunque haya tenido conocimiento de la posibilidad de que se produjeran daños o perjuicios para el cliente suscriptor.

A menudo, estas limitaciones y exoneraciones se acompañan de un compromiso del proveedor de "realizar sus mejores esfuerzos" para asegurar la máxima calidad de la prestación, entendiéndose esta calidad del servicio como una obligación de adoptar los medios necesarios para conseguirla de acuerdo con el estado de la tecnología y las prácticas del sector, y no como una obligación de obtener un concreto resultado.

Independientemente de que las acciones u omisiones que generan perjuicios en el pequeño empresario turístico sean o no sean imputables directamente al proveedor, la validez de estas exclusiones de responsabilidad dependerá en gran medida de la legislación aplicable al contrato suscrito por el pequeño empresario turístico³⁷. Si bien en el análisis realizado en capítulos anteriores nos hemos centrado

36 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*")", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

37 Recordemos que, a pesar de lo anterior, la posición jurídica del pequeño empresario turístico no es la misma que la del consumidor, con lo cual no se le aplicaría la norma de conflicto del artículo 6 del Reglamento 593/2008, de 17 de junio de 2008, sobre ley aplicable a las obligaciones contractuales, que garantiza al consumidor la protección que le otorga la ley del país de su residencia habitual. El pequeño empresario turístico que acepte la ley aplicable al contrato que le sea perjudicial en virtud del principio de autonomía de la voluntad quedará, pues, sometido a esta ley. Además, en principio no le ampara la normativa de protección al consumidor respecto de sus derechos a ejercitar acciones y a ser compensado por prestaciones defectuosas. Por nuestra parte, consideramos que puede plantearse la aplicación de la nulidad de cláusulas abusivas si el pequeño empresario se encuentra en una situación de desamparo equiparable a la de un consumidor. Ver apartado "Breve reflexión relativa a la aplicación extensiva de las normas y criterios sobre cláusulas

CAPÍTULO OCTAVO

en la cobertura del ordenamiento jurídico español, existen muchos proveedores de servicios de computación en la nube que establecen como legislación aplicable al contrato la de otro país, con lo cual, si bajo la legislación española podría discutirse su validez de acuerdo con la normativa de los artículos del Código Civil y del Código de Comercio y la Ley General de Condiciones de la Contratación, puede que otros ordenamientos permitan al proveedor exonerarse de su deber de diligencia a través de una cláusula predispuesta.

Como añadidura a lo anterior, también suelen establecerse limitaciones en el contrato respecto del ejercicio de acciones por parte del pequeño empresario suscriptor³⁸. Es habitual encontrarse no solo con daños excluidos de ser compensados (daño emergente, lucro cesante, oportunidades de negocio, etc.)³⁹, sino con la imposición de límites cuantitativos al montante de la indemnización aunque esta no cubra todas las pérdidas sufridas (por ejemplo, la suma de los importes abonados por el servicio durante un cierto período) o límites temporales u otros requisitos para poder entablar acciones de compensación⁴⁰.

La lectura y comprensión del contrato de servicios de computación en la nube es esencial para el pequeño empresario del sector turístico, observada la distribución de riesgos que generalmente efectúa el contrato predispuesto por el proveedor, claramente desventajosa para el primero. Para minimizar los riesgos derivados de la migración de datos a sistemas de computación en la nube, será necesario que el

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".

38 Ver apartado "Límites cuantitativos y temporales a las indemnizaciones por daños y perjuicios", en el capítulo "Obligaciones y responsabilidades de las partes del contrato de servicios de computación en la nube".

39 Los daños ocasionados al pequeño empresario del sector turístico pueden comprender no solo filtraciones o pérdidas de información, o perjuicios económicos derivados de la interrupción del negocio durante picos elevados de demanda, sino también la pérdida de otros activos inmateriales de gran valor para la empresa turística, como la reputación. La mayoría de proveedores de computación en la nube se eximen de compensar este tipo de daños, siempre y cuando la legislación aplicable al contrato así lo permita.

40 Como ejemplo de limitación temporal para interponer una acción de reclamación contra el proveedor, la cláusula extractada del software como servicio *Marketman*: "You acknowledge and agree that any cause of action that you may have arising out of or related to the site must commence within one (1) year after the cause of action accrues. otherwise, such cause of action is permanently barred". *MarketMan Terms of Use* [en línea]. Disponibles en: <<http://marketman.com/TermsOfUse>>. [Fecha de consulta: 12 de junio de 2017].

CAPÍTULO OCTAVO

pequeño empresario turístico adopte ciertas precauciones en materia de seguridad informática, como mecanismos de control de acceso por categorías laborales, una eficaz política de copias de seguridad y de recuperación de datos, o establecer mecanismos de cifrado de información cuando el proveedor *cloud* no los proporcione⁴¹. Asimismo, es altamente recomendable que el pequeño empresario del sector turístico se asegure de que el proveedor con quien contrata le ofrece apoyo en cuanto a implementación de hardware y software implicados en el servicio y en la migración inicial a la nube; solvente dudas sobre el manejo del programa o sobre el uso de las funcionalidades del servicio; y ofrezca servicios de soporte, consultoría técnica, etc.

3.4.- La intermediación. El socio o "*partner*" del proveedor *cloud*

Es frecuente que algunos productos no los comercialice el proveedor principal de manera directa, sino que sean los denominados "socios" o "*partners*" quienes comercialicen el software como servicio al detalle, posicionándose como intermediarios. Se tratará de una persona jurídica o un profesional que, tras realizar procesos de formación y evaluación al efecto, consigue una acreditación por parte del proveedor principal que le permite distribuir y comercializar ese software.

De manera general, el proveedor principal es el titular del servicio, al ser quien lo presta al pequeño empresario turístico y quien debe responder por su correcto funcionamiento, mientras que el intermediario presta servicios añadidos (soporte, asesoramiento, atención personalizada, gestión de incidencias, asistencia técnica, etc.) y gestiona los cobros de las cuotas devengadas por el servicio a quienes lo contratan a través de él⁴².

41 El Instituto Nacional de Ciberseguridad INCIBE recomienda a las empresas del sector turístico estas y otras acciones respecto de las plataformas informáticas utilizadas para almacenar y tratar información empresarial, con el fin de proteger la información manejada e "implementar unos buenos hábitos de seguridad". INCIBE, Nueve claves de ciberseguridad para el sector del Turismo [en línea], 2016. Disponible en: <<https://www.incibe.es/protege-tu-empresa/blog/9-claves-ciberseguridad-el-sector-del-turismo>>. [Fecha de consulta: 21 de marzo de 2017].

42 Así sucede, por ejemplo, existen integradores de soluciones en la nube, como Quonext, *partner* de Microsoft. Por ello, el software que ofrece está basado en una selección de soluciones *Microsoft Dynamics 365* y *Microsoft Dynamics NAV*, y se promocionan como expertos en gestión de soluciones en la nube para empresas del sector turístico. Como consultora, oferta los productos de

CAPÍTULO OCTAVO

Esta situación no debe confundirse con aquellos casos en los que el servicio lo presta el proveedor principal pero sustenta sus sistemas en la nube de otro proveedor. En este caso, el proveedor principal es quien presta la totalidad del servicio y quien debe responder ante el pequeño empresario turístico suscriptor, y el proveedor de capas subyacentes se posiciona como un subproveedor⁴³.

3.5.- La disponibilidad del servicio y su relevancia en picos de demanda estacionales

El sector turístico es especialmente sensible a los picos de demanda estacionales, con lo cual la computación en la nube resulta idónea para solventar problemas relacionados con los recursos limitados o infrautilizados. Al dotarse de escalabilidad y elasticidad a las capacidades de computación, el pequeño empresario del sector turístico puede hacer uso de estos servicios adecuándose a la demanda existente en cada momento. Sin embargo, estos picos de demanda estacionales a los cuales debe hacer frente el pequeño empresario del sector turístico también suponen un riesgo al migrarse información empresarial a sistemas externos que no dependen de su control, puesto que la caída del servicio puede implicar una paralización de la operativa empresarial, ante la imposibilidad de acceder a información relevante en momentos de alta demanda, con la consecuente pérdida de beneficios y efectos en su reputación empresarial.

El parámetro de la disponibilidad (o *uptime*) es un objetivo de nivel de servicio ampliamente recogido por la generalidad de softwares como servicio de nube pública de pago, modalidad de servicios ampliamente contratada por pequeños empresarios y profesionales del sector turístico⁴⁴.

Puede resultar sorprendente, especialmente para el profesional del sector

Microsoft especialmente diseñados para gestionar centros de ocio, establecimientos hoteleros, agencias de viajes, etc. para su contratación por terceros, con la certificación de Microsoft.

43 Por ejemplo, el software como servicio turístico *Appinclusive* oferta una aplicación que se sustenta en entornos en la nube de otros proveedores.

44 En otros capítulos de este trabajo se estudian otros parámetros como los compromisos en materia de seguridad, el manejo de los datos migrados por el cliente o el uso de datos personales, que también resultan importantes para el pequeño empresario turístico que contrata servicios de computación en la nube.

CAPÍTULO OCTAVO

turístico que carezca de amplios conocimientos en la materia informática⁴⁵, el hecho de que el proveedor de servicios *cloud* se comprometa a un factor de disponibilidad representado por porcentajes muy altos (generalmente abarcan del 99,5 al 99,999%) y que dejan, aparentemente, muy poco margen (menos del 1%) a caídas del sistema⁴⁶. Pero, en la práctica, el 99% de disponibilidad anual puede significar que durante más de tres días al año el servicio de computación en la nube puede no estar disponible⁴⁷. Como sabe cualquier profesional del sector, tres días sin poder acceder a su sistema *cloud* en plena temporada alta de reservas puede traducirse en una significativa pérdida de beneficios.

Por otra parte, el proveedor no incluye, generalmente, dentro del cómputo del factor de disponibilidad, cualquier periodo de tiempo en el cual el cliente no pueda acceder a los datos a los cuales tiene acceso autorizado (*downtime*). Existen ciertas excepciones comunes en los objetivos de nivel de servicio, como son las interrupciones programadas (es decir, las operaciones de mantenimiento previstas con antelación), las interrupciones breves (inferiores a 10 minutos); las provocadas por acciones o equipos del cliente o de terceros, y a factores que escapen del

45 Para este colectivo de suscriptores de servicios *cloud* en la nube pública, ciertas organizaciones han elaborado directrices de ayuda con el fin de favorecer la mejor comprensión de estos acuerdos. A modo de ejemplo, las guías del Cloud Standards Customer Council *Public Cloud Service Agreements: What to Expect and What to Negotiate*, de marzo de 2013, y la *Practical Guide to Cloud Service Agreements Version 2.0*, de abril de 2015. [En línea]. Disponibles respectivamente en: <<http://www.cloud-council.org/PublicCloudServiceAgreements2.pdf>> y <http://www.cloud-council.org/CSCC_Practical_Guide_to_Cloud_Service_Agreements_Version_2.0.pdf>. [Fecha de consulta: 21 de marzo de 2017].

46 El software como servicio *Appinclusive* informa en sus condiciones contractuales que su aplicación "se encuentra alojada en entornos *cloud* con un nivel de servicio superior al 99%".

47 Para facilitar una idea aproximada de lo que puede significar en la práctica el factor de disponibilidad, a continuación enumeramos varias correspondencias entre porcentajes indicadores del factor de disponibilidad y tiempos de caída del sistema, en cómputo anual y mensual, calculado con meses de 31 días y años de 365 días: Un factor de 99,9999% implicaría un tiempo de caída mensual de 2 segundos o anual de 24 segundos. Un factor de 99,99%, implicaría un tiempo de caída mensual de 4 minutos y 27 segundos o anual de 53 minutos y 24 segundos. Un factor de 99%, implicaría un tiempo de caída mensual de 7 horas, 26 minutos y 24 segundos o anual de 3 días, 17 horas y 16 minutos. Un factor de 98%, implicaría un tiempo de caída mensual de 14 horas, 52 minutos y 48 segundos o anual de 7 días, 10 horas y 33 minutos. Como último ejemplo, un factor de 95%, implicaría un tiempo de caída mensual de 1 día, 13 horas y 12 minutos o anual de 18 días, 14 horas y 24 minutos. Fuente de los datos: *Blogs Teoriza de Tecnología e informática*, 2011. [En línea]. Disponible en: <<http://gonzo.teoriza.com/significa-realmente-porcentaje-uptime-burbuja-disponibilidad>>. [Fecha de consulta: 21 de marzo de 2017].

CAPÍTULO OCTAVO

razonable control del proveedor⁴⁸. Además, la percepción que tenga pequeño empresario sobre la calidad del servicio *cloud* puede estar directamente relacionada con la continuidad del servicio. La falta de acceso a la información migrada en un determinado horario o fecha, o las interrupciones continuadas pueden ser susceptibles de ser consideradas como incumplimiento contractual del prestador del servicio⁴⁹. Del mismo modo, el cliente también percibe como falta de continuidad el inconveniente de tener que usar un servicio *cloud*, pero con un acceso muy lento en la ejecución de operaciones o con demasiada latencia en la transmisión por la red, lo que responde con errores a peticiones que realice el usuario, con lo cual puede resultar prácticamente inutilizable.

Sin embargo, todos los casos anteriores quedan fuera del parámetro de continuidad establecido por muchos acuerdos de nivel de servicio, porque según muchos contratos el servicio *cloud* se entiende disponible para el usuario aunque concurra alguna de las anteriores circunstancias, con lo cual el tiempo de inactividad derivado de tales incidencias no se entiende incluido dentro del porcentaje de disponibilidad al cual se ha comprometido el proveedor.

No obstante, para incluir estas incidencias dentro del acuerdo de nivel de servicio, existen otros parámetros que pueden ser de utilidad⁵⁰, como el porcentaje de peticiones exitosas⁵¹ o el porcentaje de peticiones de aprovisionamiento entregadas puntualmente⁵². Sin embargo, no todos los proveedores recogen en sus contratos

48 Estos ejemplos han sido extractados del acuerdo de nivel de servicio del software como servicio (SaaS) *Microsoft Dynamics CRM*. [En línea]. Disponible en: <<https://port.crm.dynamics.com/portal/static/1033/sla.htm>>. [Fecha de consulta: 20 de marzo de 2017].

49 Por ejemplo, una serie de cortes de suministro *cloud* breves pero continuados a modo de intermitencia pueden implicar para el cliente falta de disponibilidad del servicio (por ejemplo, un hotel que utilice una herramienta de CRM o *Customer Relationship Management* para atender a clientes) y, sin embargo, no alcanzar el mínimo para que devenguen penalización para el proveedor, porque se vayan repitiendo a lo largo de diferentes meses o porque cada una de las interrupciones sea inferior a 10 minutos.

50 *Digital Agenda for Europe*, en concreto la Cloud Computing European Strategy, en sus directrices. *Cloud Service Level Agreement Standardisation Guidelines* [en línea], pág. 15. Disponible en: <<https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>>. [Fecha de consulta: 21 de marzo de 2017].

51 Porcentaje de peticiones exitosas. Describe el número de peticiones procesadas sin errores por el servicio sobre el número total de peticiones, expresadas en modo de porcentaje. *Cloud Service Level Agreement ...*, *op. cit.*, pág. 15.

52 Peticiones de aprovisionamiento entregadas puntualmente. Describe el número de peticiones de

CAPÍTULO OCTAVO

estos parámetros complementarios.

Tanto la disponibilidad como el resto de parámetros son a menudo monitorizados por el proveedor, no solo para controlar que está cumpliendo con los mínimos asumidos en el acuerdo de nivel de servicio, sino también para tomar decisiones relacionadas con la infraestructura (agregar más hardware, ajustar la asignación de recursos, etc), su estrategia empresarial y el estado de la técnica. A menudo, los proveedores de servicios *cloud* sujetos a acuerdos de nivel de servicio ponen a disposición del cliente las mediciones efectuadas e informan de eventuales interrupciones en el suministro⁵³.

Por otra parte, es razonable pensar que debería ofrecerse al cliente la posibilidad de realizar pruebas de medición del nivel de desempeño del servicio, ya sea con herramientas facilitadas por el propio proveedor, ya sean proporcionadas por terceros. El suscriptor también puede usar esa información periódica sobre los resultados de las mediciones de disponibilidad y rendimiento del servicio para optimizar el uso de los servicios suscritos. Además, puede valorar opciones sobre precios y beneficios del servicio contratado o de servicios adicionales o compararlos con servicios proporcionados por otros proveedores.

3.6.- Suspensión y terminación del contrato. Efectos

El pequeño empresario del sector turístico debe ser consciente de que el proveedor a menudo se reserva el derecho a interrumpir el servicio o denegarle el acceso, sin necesidad de aviso previo y a su libre discreción, en caso de que incumpla el contrato, por ejemplo, cuando se retrase en el pago de las cuotas o efectúe un uso inadecuado del servicio. Dependiendo de lo establecido en el resto de cláusulas y del

aprovisionamiento completadas de manera puntual sobre el número total de peticiones de aprovisionamiento, expresadas en modo de porcentaje. Estas últimas pueden variar considerablemente dependiendo del tipo de servicio considerado. Directrices. CLOUD COMPUTING EUROPEAN STRATEGY, *Cloud Service Level Agreement ...*, *op. cit.*, pág. 15.

53 Sirva de ejemplo la *G-Suite Status Dashboard*, una tabla de información accesible desde el sitio web del proveedor *Google* que proporciona datos actualizados sobre el rendimiento del software como servicio *Google G-Suite*, determinando la hora en la cual ha tenido lugar una interrupción y el estado de recuperación del sistema. Disponible en: <<https://www.google.com/appsstatus#hl=es&v=status>>. [Fecha de consulta: 21 de marzo de 2017].

CAPÍTULO OCTAVO

motivo de la extinción del servicio, podrá accederse o no a una indemnización por cancelación anticipada.

En caso de que sea el pequeño empresario quien decida terminar con el contrato de servicios *cloud*, es recomendable que verifique si su cancelación anticipada del contrato implica la renuncia a las cuotas adelantadas por el uso del servicio, o si tiene opción de recuperar su importe.

Por otra parte, cuando el contrato se termina, el cliente debe conocer cuál será el destino de los datos migrados. Así, por una parte, debe asegurarse de que el contrato establezca la posibilidad de recuperación de los datos migrados, para poder transmitirlos al sistema de otro proveedor *cloud* o para instalarlos en su propio equipo. Por otra parte, es recomendable que ese informe sobre el proceso aplicado a las copias o replicados de esos datos remanentes en sistemas del proveedor, y saber si posteriormente serán inutilizados, borrados progresivamente o destruidos de los sistemas en los cuales están almacenados, y el tiempo aproximado que durará este proceso hasta que los datos remanentes se conviertan en irrecuperables⁵⁴.

4.- LA PROTECCIÓN DE DATOS PERSONALES APLICADA A PEQUEÑOS EMPRESARIOS DEL SECTOR TURÍSTICO USUARIOS DE SERVICIOS *CLOUD*

La mayor parte de la actividad empresarial turística inevitablemente implica el tratamiento de datos personales de terceros, sean estos clientes, empleados u otros (profesionales externos, etc.). Por ejemplo, en un establecimiento de alojamiento se manejan datos de clientes al realizarse reservas y cancelaciones, almacenarse en archivos digitales documentos físicos con información personal necesarios para efectuar el registro (documentos identificativos, tarjetas de crédito, etc.), al comunicar información personal a través de correos electrónicos, al utilizar datos personales para actividades de promoción o fidelización, etc.

Además, tampoco resulta extraño que empresas turísticas que desempeñan

54 El proveedor del software como servicio *Appinclusive* permite al pequeño empresario recuperar una copia digital de los datos migrados. para lo cual dispone de 30 días, y se compromete a destruirlos una vez finalizado el contrato.

CAPÍTULO OCTAVO

actividades muy similares traten información diferente, debido a que el turista se decanta cada vez más por servicios altamente personalizados y adecuados a sus gustos y preferencias personales⁵⁵.

Dentro del tratamiento de datos personales, existen ciertas cuestiones en materia de privacidad con las cuales el pequeño empresario del sector turístico usuario de servicios de computación en la nube debe tener especial cautela. A continuación, nos detendremos brevemente en las que, a nuestro parecer, son más significativas.

4.1.- El pequeño empresario turístico como responsable del tratamiento. La importancia de la finalidad del tratamiento y del consentimiento previo e informado

El responsable del tratamiento es aquella persona física o jurídica que decida sobre el uso y la finalidad del tratamiento de datos personales facilitados por el interesado; en cambio, los encargados del tratamiento tratan datos por cuenta del responsable (art. 2 Directiva 95/46/CE, art. 3.3 LOPD, art. 4 RGPD)⁵⁶.

Debe recordarse que la empresa turística es quien decide, generalmente, recabar de terceros cierta información personal, para poder proceder al tratamiento de esa información que resulte necesario para prestar el servicio turístico. Igualmente, decide sobre la finalidad que tendrá ese tratamiento: mejora de la personalización del servicio, publicidad y promoción, cesión a otras compañías de servicios relacionados con la actividad principal, almacenamiento y registro, etc. En estos casos, pues, el pequeño empresario (persona jurídica) está actuando como

55 Por ejemplo, los servicios turísticos que adaptan sus menús a alergias, intolerancias o ideología religiosa, o necesitan disponer de información respecto si los clientes son personas con movilidad reducida o tienen alguna otra discapacidad, o los establecimientos "*gay friendly*" o enfocados al turismo de salud y bienestar; cuando para prestar el servicio turístico almacenen información sensible de manera que sea fácilmente asociable a los datos de identificación de una persona física, deberán adoptar medidas de seguridad de nivel alto. Sin embargo, otros servicios de alojamiento o restauración no tratarán datos especialmente sensibles, con lo cual serán suficiente que adopten medidas de seguridad de nivel medio.

56 Ver apartado "La asignación de los roles de titular de los datos, responsable y encargado del tratamiento en la computación en la nube", en el capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

CAPÍTULO OCTAVO

responsable del tratamiento de los datos facilitados por sus clientes, aunque estas operaciones de tratamiento se realicen a través del uso de servicios de computación en la nube y el almacenamiento de esos datos personales o las herramientas de procesamiento utilizadas provengan de otros proveedores.

Asimismo, será necesario que el pequeño empresario turístico, como responsable del tratamiento, informe al interesado sobre las finalidades a las cuales pretende destinar la información, especialmente si estas finalidades exceden del objeto contractual que fundamente la relación jurídica empresario turístico-interesado.

En la relación jurídica entre el proveedor de servicios *cloud* y el empresario turístico suscriptor de estos servicios, el proveedor *cloud* se considerará un mero encargado del tratamiento, mientras que sobre el empresario turístico recaerá toda la responsabilidad por los datos personales de terceros que migre a la nube para proceder, con ayuda de las funcionalidades suministradas, a todo o parte de su tratamiento automatizado (Dictamen 5/2012 del Grupo de Trabajo del Artículo 29)⁵⁷. Entre ambos mediará un contrato que regule el tratamiento de los datos migrados por parte del proveedor *cloud*, para dar cumplimiento a la normativa sobre privacidad (art. 12.2 LOPD, art. 28.3 RGPD).

El sector turístico maneja una ingente cantidad de datos de carácter personal tanto de clientes y consumidores (datos de identificación y facturación, preferencias y gustos, imágenes y voz captadas mediante mecanismos de videovigilancia o similares, etc.) como de personal empleado (currículums, datos sobre seguridad social, datos bancarios, datos sobre personalidad y comportamiento, datos sobre reconocimientos o certificados médicos, etc.) y de proveedores (generalmente, datos de contacto de nivel básico)⁵⁸.

57 A pesar de esta calificación del empresario suscriptor de servicios *cloud* como responsable, debe tenerse en cuenta su capacidad de control efectivo sobre el tratamiento, por lo que será sumamente necesario que el proveedor permita al responsable el cumplimiento de sus obligaciones legales, y le facilite las herramientas para ello. Ver apartado "El responsable del tratamiento y sus obligaciones", en el capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

58 Especialmente en lo referente a información sobre clientes y empleados, también es importante recordar que existen otros aspectos a tener en cuenta en materia de protección de datos, aunque queden fuera de nuestro objeto de estudio, como imágenes obtenidas mediante cámaras de seguridad o dispositivos biométricos, información personal almacenada en soportes físicos (como

CAPÍTULO OCTAVO

El pequeño empresario turístico, como responsable del tratamiento, debe informar al interesado de que sus datos serán objeto de tratamiento (art. 5 LOPD, arts. 13 y 14 RGPD), y recabar el consentimiento expreso y por escrito de los titulares de tales datos personales sensibles y restringir su tratamiento a la finalidad para la cual se recabaron (art. 6 LOPD, arts. 6 y 7 RGPD)⁵⁹. Aquella información personal recogida con una concreta finalidad (uso de los servicios únicamente para un evento o actividad puntual, etc.) debe realmente restringirse a esa única finalidad, y deben evitarse aquellos tratamientos que tengan fines de los cuales no se hubiera informado adecuadamente a cada interesado, hasta que se obtenga el pertinente consentimiento. Cabe destacar que, según la Agencia Española de Protección de Datos, los tratamientos que tengan por objeto elaborar perfiles personales o segmentaciones con fines comerciales suponen un tratamiento ajeno a la relación negocial con el cliente, con lo cual deberá recabarse un consentimiento específico para poder efectuar el tratamiento con tal finalidad, y, además, debe permitirse al interesado oponerse a este tratamiento en el momento de recogida de la información, por ejemplo, mediante la marcación de una casilla en el formulario facilitado para la prestación del consentimiento informado⁶⁰.

Por otra parte, cuando el encargado del tratamiento, en nuestro caso el proveedor *cloud*, destine los datos a otra finalidad diferente a aquella por la cual el empresario turístico que los recabó le facilitó esos datos, será considerado responsable del tratamiento a efectos de la determinación de infracciones y la imposición de sanciones (art.12.4 LOPD, art. 28.10 RGPD).

Con la normativa de aplicación actual, es decir, la LOPD, no es necesario que informe y obtenga el consentimiento del titular respecto de migraciones de datos a sistemas en la nube, ya que el proveedor *cloud* se considera un encargado del tratamiento y, por tanto, no nos hallamos ante una comunicación de datos (tal y

formularios en papel o tarjetas de acceso a diferentes estancias o servicios). De acuerdo con el principio de calidad de los datos, la recogida de datos debe ser proporcionada, y que el uso de esos datos debe restringirse a la finalidad con la cual se recogieron (arts. 4 LOPD, 8 RLOPD y 5 RGPD).

59 Agencia Española de Protección de Datos. AEPD, *Plan de inspección de oficio a cadenas hoteleras* [en línea], 2004, pág. 25. Disponible en: <<https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/RECOMENDACIONESCADENASHOTELERASDEFINITIVAS.pdf>>. [Fecha de consulta: 24 de marzo de 2017].

60 Agencia Española de Protección de Datos. AEPD, *Plan de inspección...*, *op. cit.*, pág. 26.

CAPÍTULO OCTAVO

como considera el artículo 12.1 LOPD)⁶¹. Pero cuando se aplique el nuevo Reglamento europeo (a partir del 25 de mayo de 2018) será necesario que el titular de los datos personales sea adecuadamente informado y 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 a la posibilidad de que se produzca tal transferencia, deberá ser igualmente informado de las garantías legales de esa transferencia, de acuerdo con el artículo 13. 1.f) del Reglamento europeo⁶². Por ello, será necesario conocer si el proveedor de servicios de computación en la nube aloja los datos migrados por el pequeño empresario en servidores fuera del Espacio Económico Europeo que no ofrezcan un nivel adecuado de garantías según los criterios de la Comisión Europea.

El pequeño empresario turístico suscriptor de servicios *cloud* que impliquen transferencias internacionales de datos, al ser considerado responsable del tratamiento, deberá estar en situación de probar que el titular de los datos ha facilitado este consentimiento y, en aquellos casos en los que se recabe mediante una declaración escrita que abarque otras informaciones, será necesario que la prestación del consentimiento se distinga claramente de otros asuntos (art. 7 RGPD)⁶³.

Nuestra recomendación al pequeño empresario turístico es que, al recabar los datos y el consentimiento del interesado, en la información a suministrarle, en

61 Artículo 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".

62 Artículo 13.1.f del Reglamento General de Protección de Datos. "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: (...) en su caso, la intención del 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". En el caso en el que el pequeño empresario turístico realice partes del tratamiento de datos personales mediante sistemas de computación en la nube, deberá informar sobre esta cuestión al titular cuyos datos personales se recaben, así como la existencia del acuerdo *Shield* como garantía de tal transferencia.

63 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. 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento".

CAPÍTULO OCTAVO

cualquier caso, incluya la posibilidad de que los datos podrán ser tratados mediante sistemas de computación en la nube, y de la posibilidad de que se efectúen debido a ello transferencias internacionales de datos, junto con las garantías legales de tales transferencias, porque, aunque en el momento de redacción de este trabajo esta información no sea estrictamente necesaria, sí resultará exigible una vez que sea aplicable el nuevo Reglamento europeo. Asimismo, recomendamos al pequeño empresario que ponga especial atención en la elección del proveedor *cloud*, para asegurar el cumplimiento del nuevo Reglamento europeo.

A continuación, nos detendremos brevemente sobre la cuestión de las transferencias internacionales que tienen lugar mediante la prestación de servicios de computación en la nube a pequeños empresarios del sector turístico.

4.2.- La transmisión de datos personales a terceros a través de servicios *cloud*

La gestión de actividades turísticas generalmente implicará un intenso tráfico de información de clientes y empleados entre diferentes profesionales y empresas (turoperadores, agencias de viajes, asesorías externas, mutuas de salud, etc.), con lo cual deberá haberse solicitado el consentimiento del titular de los datos de manera previa e informada, cumpliendo con el deber de información al cliente sobre la posibilidad de cesiones de datos y accesos por cuenta de terceros (arts. 11 y 12.3 LOPD, 20 a 23 RLOPD y 13.1.e RGPD).

Actualmente, la mayoría de esta información se transmite a través de medios telemáticos, (aplicaciones informáticas, correo electrónico, sistemas automatizados ERP o CRM, etc.), siendo común que estos medios se presten en forma de servicios de computación en la nube. Si bien no será necesario informar al cliente del uso de estos servicios como mecanismo de transmisión, sí deberá cumplir con los requisitos de información respecto de cesiones de datos, como hemos dicho. Asimismo, es recomendable adoptar ciertas precauciones respecto de funcionalidades como la compartición de archivos dentro del mismo servicio *cloud*, especialmente si estos archivos digitales incorporan datos de terceros.

Cuando el empresario turístico utilice sistemas de tratamiento de datos que

CAPÍTULO OCTAVO

permitan la sincronización y la elaboración de perfiles de los clientes basados en sus gustos, preferencias o servicios solicitados o contratados, será recomendable que recabe el consentimiento del titular de los datos respecto de esta concreta finalidad⁶⁴.

4.3.- Transferencias internacionales de datos personales

Hemos mencionado que al recabarse información personal de terceros para proceder a su tratamiento, es necesario que el titular de los datos personales haya prestado previamente su consentimiento para las finalidades necesarias para que el empresario turístico, como responsable del tratamiento, pueda proceder a este. Cuando el uso de servicios de computación en la nube por el empresario turístico implique transferencias de datos personales fuera del territorio español y que tengan por destino países que no cuenten con las garantías de nivel de protección adecuado según la Comisión Europea (arts. 25 y 26 LOPD, arts. 44 y ss. RGPD)⁶⁵, el responsable del tratamiento deberá asimismo informar al cliente de manera transparente y previa, y recabar su consentimiento de manera que constituya una prueba⁶⁶.

La información que pueda facilitar el proveedor *cloud* al empresario del sector turístico sobre la ubicación de los servidores que pueden almacenar datos de su empresa es relevante, con el fin de determinar el procedimiento necesario para adecuar las transferencias de información personal a la legalidad, ya que los servidores que almacenan la información, como se sabe, pueden encontrarse en países diferentes al del establecimiento del proveedor de servicios *cloud* con quien se contrata.

Respecto de transferencias internacionales a EE.UU., país donde se encuentran muchos de los servidores de los principales proveedores de servicios de computación en la nube, cabe recordar que existe un acuerdo entre EE.UU. y Europa

64 Así lo recomendó en su momento la Agencia Española de Protección de Datos. AEPD, *Plan de inspección...*, *op. cit.*, pág. 23.

65 Ver apartado "Localización y seguridad de los datos. Acceso a datos por terceros, cesiones de datos y transferencias internacionales", en el capítulo "Privacidad en la nube: principales cuestiones de carácter personal".

66 Ver apartado "Transferencias internacionales de datos y *Cloud Computing*", en el capítulo "Privacidad en la nube: principales cuestiones sobre protección de datos de carácter personal".

CAPÍTULO OCTAVO

que ha permitido la exportación de datos de ciudadanos europeos, el denominado acuerdo *Shield* o "Escudo de Privacidad", que substituye al anterior acuerdo *Safe Harbor* o "Puerto Seguro".

Como se ha visto en anteriores capítulos de este trabajo, para que una transferencia internacional de datos sea legal, de acuerdo con la legislación aplicable actualmente debe someterse a diferentes requisitos (art. 33 LOPD), entre ellos el mencionado cumplimiento del deber de información o la notificación de la transferencia a la Agencia Española de Protección de Datos (art. 34 LOPD) y la obtención de la autorización pertinente. Deberemos esperar a eventuales modificaciones legislativas de adaptación al nuevo Reglamento europeo para averiguar si esta exigencia se mantiene.

Puesto que los clientes de servicios en la nube son los responsables de la seguridad e integridad de los datos que tratan, aunque estos se encuentren fuera de las instalaciones empresariales y estén gestionados por un proveedor en la nube, es recomendable para el empresario turístico español que contrate con un proveedor que permita que el marco legal de los datos sea el de un país que ofrezca un nivel adecuado de protección, según los criterios de la Comisión Europea⁶⁷. Cuando esto no sea posible, deberá suscribir con el proveedor las cláusulas contractuales tipo adoptadas por la Comisión Europea a tal efecto o las normas corporativas vinculantes (si procede), o recabar una autorización previa del Director de la Agencia Española de Protección de Datos⁶⁸. En caso contrario, podría ser sancionado por la Agencia Española de Protección de Datos, si bien, de momento, no nos consta que se hayan iniciado procedimientos sancionadores de la Agencia por este motivo.

4.4.- Referencias en el documento de seguridad a los sistemas *cloud*

Es obligación del empresario turístico que trate datos personales de terceros,

67 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_ame_nazas_en_cloud_computing.pdf>. [Fecha de consulta: 16 de marzo de 2017].

68 GUASCH PORTAS, Vicent; SOLER FUENSANTA, José; " *Cloud Computing*, turismo y protección de datos", *Revista de Análisis Turístico*, núm. 17, 2014, pág. 67.

CAPÍTULO OCTAVO

como responsable del tratamiento, la adopción de medidas técnicas y organizativas para garantizar la seguridad de esos datos (art. 9 LOPD, art. 5.1.e RGPD). Las medidas de seguridad implementadas en la empresa o que adopte el profesional turístico deben recogerse en el documento de seguridad que exige el Reglamento de Desarrollo de la LOPD en su artículo 88⁶⁹. El documento de seguridad se adaptará al nivel de seguridad previsto según los datos objeto del tratamiento sean datos de nivel bajo, medio o alto. En nuestra opinión, y cuando los servicios turísticos puedan involucrar datos de carácter sensible (salud, afinidad con determinadas ideologías, etc.), es altamente recomendable para el pequeño empresario que lleve a cabo tales actividades que adopte medidas de nivel alto, especialmente si prevé que estos datos se alojarán en servidores remotos de un proveedor de servicios de computación en la nube.

Asimismo, es recomendable que se integre en el documento de seguridad un registro actualizado de los usuarios que tengan acceso al sistema *cloud* de gestión de información que almacene datos personales (CRM, ERP, etc.), y que los sistemas que permitan autenticar a los usuarios garanticen una clave de acceso personal e intransferible para cada usuario, e impidan acceder a información no necesaria para el desempeño de sus funciones. Es preferible que únicamente ciertos cargos autorizados según el documento de seguridad tengan entre sus funciones la concesión, alteración o revocación de credenciales o accesos a los archivos que contengan los datos digitales.

Igualmente, deben incorporarse, en el registro de incidencias que forma parte del documento de seguridad (art. 88.3 RLOPD), aquellos contratiempos que hayan podido acontecer en el uso de las herramientas de computación en la nube, mencionando el tipo de incidencia, fecha y hora, qué usuario lo ha detectado, a quién se le ha notificado y cuales han sido las consecuencias del incidente, y el procedimiento de recuperación de datos utilizado, así como otras medidas paliativas⁷⁰.

69 El Plan de inspección de oficio de la AEPD, realizado en 2004, observó entonces algunas deficiencias comunes en los documentos de seguridad de establecimientos hoteleros, tales como la falta de detalle en la función asignada a cada trabajador y sus obligaciones concretas respecto del tratamiento, falta de mecanismos de autenticación que protejan el acceso a datos personales o la falta de medidas que protejan los lugares físicos y los servidores donde se almacenan los datos. AEPD, *Plan de inspección...*, *op. cit.*, pág. 15.

70 Así lo recomendó, aunque de manera genérica y sin referencia a la computación en la nube

CAPÍTULO OCTAVO

4.5.- Destrucción, inhabilitación o borrado de información personal almacenada en la nube

Las empresas dedicadas al sector turístico deben tener una especial cautela en cuanto al destino de los datos de clientes una vez finalizada la relación que los vinculaba (alojamiento, transporte, productos de ocio, etc.). Si bien existen normas jurídicas que obligan al pequeño empresario a conservar ciertos datos en sus archivos históricos, es habitual que muchos otros datos personales se mantengan activos en los sistemas de gestión de la actividad empresarial durante un tiempo indefinido, incluso tras largos periodos en los cuales ese cliente no ha vuelto a utilizar los servicios de la empresa turística o expiradas las mencionadas obligaciones de conservación de información.

Es recomendable que la propia empresa turística establezca procedimientos internos que permitan identificar qué datos personales es necesario mantener activos en el fichero de gestión y cuáles deben almacenarse en ficheros históricos (como ejemplos de obligaciones de conservación de información sobre facturación, o llevanza del libro-registro y partes de entrada de viajeros). Además, es conveniente que el pequeño empresario determine un período de tiempo durante el cual los datos personales que ya no resultan necesarios pueden bloquearse y, posteriormente, cuando no ya esté justificada su retención, suprimirse de manera definitiva⁷¹.

Para ello, debe utilizarse un sistema de destrucción, inhabilitación o borrado de datos migrados a la nube que permita dar pleno cumplimiento a lo exigido por la normativa en materia de privacidad⁷².

Una vez cumplido el objetivo del tratamiento de los datos personales, finalizada la prestación de servicios turísticos o la relación laboral, y cuando no existan sobre tales datos obligaciones legales que exijan su conservación, estos datos deberían bloquearse o suprimirse, especialmente si son altamente sensibles, como sucede con los datos de salud (por ejemplo, alergias alimentarias, necesidades

(puesto que en esos momentos la tecnología *cloud* era todavía joven) la Agencia Española de Protección de Datos. AEPD, *Plan de inspección...*, *op. cit.*, págs. 23, 34.

71 Así lo recomendó en su momento la Agencia Española de Protección de Datos. AEPD, *Plan de inspección...*, *op. cit.*, pág. 24.

72 Respecto de los diferentes sistemas de borrado de datos en la nube, ver apartado "Las técnicas de borrado de contenidos en la nube y sus garantías", en el capítulo "Suspensión, modificación y extinción del contrato de servicios de computación en la nube".

CAPÍTULO OCTAVO

especiales de clientes con problemas de movilidad o salud, etc.) ideología, afiliación sindical, religión o vida sexual (por ejemplo, al reservarse servicios turísticos especialmente orientados a personas con tendencias o ideologías similares, u organización de eventos que permitan asociar información de este tipo con las personas físicas asistentes) y estos datos se almacenan en la nube.

Los datos facilitados al pequeño empresario turístico únicamente podrán tratarse para las finalidades sobre las cuales ha sido informado y ha consentido el interesado, y una vez que no sean necesarios para cumplir esta finalidad, deberán "eliminarse" de los sistemas donde estén almacenados. Igualmente, debe recordarse que el consentimiento del titular de los datos es revocable, en cuyo caso deberán "borrarse" de los sistemas o herramientas en la nube la información personal afectada por el ejercicio de sus derechos como titular, pudiendo solicitarse para ello la colaboración del proveedor, para que el responsable del tratamiento pueda atender a esta petición dentro del plazo legalmente determinado⁷³.

Tras lo anterior, nos sumamos a la opinión de otros autores al afirmar que aquel empresario del sector turístico que pretenda aprovechar los beneficios de la computación en la nube debe garantizar que el proveedor elegido colabore y cumpla con la normativa en materia de protección de datos. En caso contrario, lo más sensato es no efectuar "el salto a la nube", debido al elevado importe de las sanciones que conlleva el incumplimiento de la normativa sobre privacidad, y gestionar el establecimiento o servicio turístico a través de software tradicional que esté instalado en los ordenadores o servidores del propio empresario⁷⁴. Otras modalidades de implementación también pueden tenerse en cuenta (nube privada, híbrida, etc.), si bien deberá valorarse el coste económico por parte del pequeño empresario.

73 Respecto del borrado de datos, ver apartado "Los efectos de la finalización del contrato de servicios de computación en la nube sobre los datos personales", en el capítulo "Privacidad en la nube: principales cuestiones de protección de datos de carácter personal".

74 La Ley Orgánica de Protección de Datos distingue entre infracciones leves, graves y muy graves. Las sanciones varían dependiendo de la categoría de infracción cometida, y comprenden desde el apercibimiento hasta importes cuya cuantía abarca desde los 900 a los 600.000 euros, según establece el artículo 45 de la LOPD.

5.- WEB 2.0 EN EL SECTOR TURÍSTICO: ASPECTOS JURÍDICOS ANÁLOGOS A LA CONTRATACIÓN DE SERVICIOS *CLOUD*

Algunas plataformas web soportadas por tecnología *cloud* han supuesto un enorme impacto en el sector, cambiando el "ecosistema económico" y dando mucha más participación al usuario y a su valoración de la experiencia sobre el producto o servicio turístico disfrutado⁷⁵. Estas Webs 2.0 permiten al internauta crear y compartir contenidos a través de interfaces sencillas, y no siempre es sencillo distinguir las del modelo comercial del software como servicio gratuito⁷⁶.

Existen en la actualidad múltiples Webs 2.0 de diferentes categorías y con distintas funcionalidades: buscadores, comparadores, foros para compartir y valorar experiencias, etc.⁷⁷. Algunas de estas plataformas, además, posicionan a las empresas y establecimientos turísticos de acuerdo con las valoraciones de los usuarios u otros mecanismos, y, a su vez, permiten realizar reservas o adquirir servicios turísticos de las mismas. A continuación, comentaremos brevemente algunos aspectos jurídicos en el ámbito de las plataformas Web 2.0, y las similitudes existentes con los servicios de computación en la nube.

5.1.- Algunos aspectos jurídicos de los contratos predispuestos por comparadores de servicios turísticos

Los proveedores de Webs 2.0 sujetan a la aceptación de ciertas condiciones el uso de sus plataformas. Las Webs 2.0 relacionadas con el sector turístico tienen distintas finalidades, dependiendo del servicio, y generalmente se utilizan para

75 Algunos portales, como *TripAdvisor* o *Booking*, han cambiado completamente el "ecosistema económico" del sector turístico, y dan al usuario una mayor participación, al permitirle valorar la experiencia y el producto final. PALOS SÁNCHEZ, Pedro; AGUAYO CAMACHO, Mariano; *Los ecosistemas de turismo...*, op. cit., pág. 136.

76 Ver apartado "Qué no es *Cloud Computing: Web 2.0*", en el capítulo "Concepto y características técnicas de la computación en la nube".

77 Como ejemplo de una Web 2.0 que integra múltiples funcionalidades, podemos mencionar *Minube*. Esta plataforma se describe como "una comunidad de viajeros" que integra un comparador de precios de vuelos, alquileres de coches y hoteles, una red social que permite crear un perfil con gustos y preferencias y compartir las experiencias de viajes con otros usuarios. También permite a las empresas mejorar su posicionamiento.

CAPÍTULO OCTAVO

reunir información sobre viajes, realizar reservas, comparar precios, publicar opiniones y compartir experiencias. En ocasiones se entienden aceptadas por el mero uso del sitio web, y en otras se advierte al internauta que no está autorizado a abrirse una cuenta de usuario y utilizar estas funcionalidades si no está de acuerdo con todas las condiciones⁷⁸.

Como también sucede en la mayoría de acuerdos de servicios prestados a través de Internet, como los servicios de computación en la nube pública, en muchas condiciones generales el proveedor de la plataforma web se reserva la facultad de modificar las condiciones legales, así como los contenidos o las funcionalidades de la plataforma, en cualquier momento y sin necesidad de previo aviso⁷⁹. Por ello es recomendable que el usuario revise eventuales modificaciones en la versión del acuerdo legal antes de proceder a prestar su consentimiento, y que el proveedor destaque la fecha de la última modificación y, a ser posible, averigüe los contenidos que han sido modificados.

A continuación, destacaremos algunos de los aspectos contractuales (sin distinguir entre términos de uso del servicio por usuarios particulares o por profesionales) que se asemejan a la contratación de servicios de computación en la nube, y otros aspectos que son específicos de estas plataformas.

5.1.1.- Políticas de uso adecuado y veracidad de los contenidos compartidos por el usuario

Al igual que sucede en los servicios de computación en la nube, los usuarios de Webs 2.0 se comprometen a usar el servicio de manera ética y leal. Por ello, los contratos de estas plataformas también incorporan las denominadas políticas de uso adecuado (PUA), un conjunto de cláusulas que prohíben ciertos usos y abusos de los

78 A modo de ejemplo, véanse los términos de servicio de las plataformas *TripAdvisor*, *Minube* y *Booking*. Disponibles respectivamente en: <<https://tripadvisor.mediaroom.com/ES-terms-of-use>>, <<http://www.minube.com/politica-privacidad-canon>> y <<http://www.booking.com/content/terms.es.html>>. [Fecha de consulta: 22 de marzo de 2017].

79 Como ejemplo, la reserva efectuada por el comparador *Rastreator.com*: "*Rastreator.com* se reserva el derecho a modificar en cualquier momento y sin necesidad de previo aviso la presentación, configuración y contenidos de la website de *Rastreator.com*, así como el presente "Aviso Legal", como cualesquiera otras particularidades que acaso existieren para determinados espacios, servicios o usos. Por este motivo, *Rastreator.com* recomienda a los usuarios que lean detenidamente el "Aviso Legal" y "Política de Privacidad" con anterioridad a que acepten la casilla para prestar su consentimiento". Aviso legal disponible en: <<http://www.rastreator.com/aviso-legal.aspx>>. [Fecha de consulta: 23 de marzo de 2017].

CAPÍTULO OCTAVO

contenidos y funcionalidades proporcionados por el servicio (por ejemplo, la publicación de mensajes de contenido sexual, difamatorio, ofensivo u obsceno; la publicación de datos de contacto de terceros, la difusión de *spam* o *malware* utilizando la plataforma, sobrecargar el servicio, etc.)⁸⁰. Si bien los proveedores de estas plataformas suelen afirmar que eliminarán los contenidos de aquellos usuarios que no cumplan con estas políticas (a su entera discreción y sin establecerse procedimientos de réplica por parte del usuario)⁸¹, también suelen incorporar en sus condiciones una exención de responsabilidad ante terceros respecto de tales infracciones⁸².

80 El comparador de sitios webs de reserva *Trivago* establece en sus términos de uso las siguientes obligaciones para los usuarios respecto del uso del servicio: "Es responsabilidad de los usuarios adquirir los derechos sobre los contenidos (texto, fotografías, opiniones, enlaces, etc.) que añadan a *Trivago*, lo que significa que deben asegurarse de poseer todos los derechos sobre los contenidos que publiquen en la plataforma de *Trivago* y de que estos contenidos no violen los derechos de terceros. Los usuarios se comprometen a no utilizar los servicios de *Trivago* para crear los siguientes tipos de contenidos: publicidad encubierta; contenidos no relacionados con el elemento sobre el que se está opinando; contenidos subjetivos o intencionadamente falsos; contenidos inmorales, pornográficos u ofensivos; contenidos que infrinjan los derechos de terceros y, más concretamente, los derechos de autor; contenidos que sean contrarios a la ley vigente o constitutivos de delito; contenidos infectados con virus u otros programas que puedan dañar el software o el hardware o que puedan afectar al correcto uso y/o funcionamiento de los ordenadores; encuestas o cartas en cadena; y contenidos que tengan como objetivo recoger o usar los datos personales de otros usuarios, especialmente para fines comerciales. Los usuarios se comprometen a no usar programas o funciones para la generación automática de opiniones o contenidos en *Trivago*". Asimismo, establece que "en caso de incumplimiento del presente contrato de términos y condiciones, *Trivago* se reserva el derecho a eliminar el contenido sin necesidad de declarar los motivos, a retener los pagos obtenidos en la Comunidad de *Trivago* y a bloquear permanentemente al miembro en cuestión. Esto no afectará al derecho a incoar una causa penal". Términos del servicio disponibles en: <<http://company.trivago.es/terms-of-service/>>. [Fecha de consulta: 22 de marzo de 2017].

81 La plataforma *Trivago* afirma que "en caso de que se ponga en conocimiento de *Trivago* que un miembro está haciendo un uso inadecuado de su web, *Trivago* podrá retirar el acceso al usuario y eliminar su registro en el plazo de una semana tras recibir la información. El usuario también podrá cancelar su propio acceso y registro dentro del mismo plazo. Lo anterior no afectará al derecho a la resolución inmediata por una causa justificada". [Fecha de consulta: 23 de marzo de 2017].

82 *Minube* se compromete a eliminar los contenidos que infrinjan las prohibiciones establecidas por las términos de uso: "*Minube* se reserva el derecho de no publicar aquéllos contenidos que resulten contrarios a las presentes normas, así como retirar todo artículo o comentario publicado que no se ajuste a las mismas, sin notificación de ninguna clase. *Minube* se reserva el derecho de cancelar el registro y entrada a la comunidad de viajeros en la medida que determinados usuarios reincidan en este tipo de conductas (...). Por ello serán eliminados de *Minube* los perfiles de usuarios que contengan: lenguaje o sugerencias de tipo sexual, fotografías sexualmente sugerentes, contenido difamatorio, abusivo, agresivo o violento, lenguaje ofensivo u obsceno", aunque también afirma que, si bien "periódicamente se realizan exhaustivos controles para asegurar que se cumplen las políticas y se mantiene la calidad de lo publicado", no se responsabiliza por esos contenidos: "dado que es imposible que *Minube* pueda controlar todos los contenidos publicados, no puede asumir la responsabilidad sobre los mismos. Cualquier usuario que proporcione información o realice actividades que contravengan la legalidad vigente asumirá la responsabilidad exclusiva de los perjuicios y consecuencias derivadas de la misma, eximiendo a *Minube* de cualquier responsabilidad". [Fecha de

CAPÍTULO OCTAVO

5.1.2.- Propiedad intelectual de los contenidos creados por el usuario

Es habitual que, a la vez que se reconoce la propiedad intelectual de los contenidos creados por el usuario a este último, se incluyan en las cláusulas contractuales cesiones de estos derechos en favor de la plataforma. Estas licencias, al igual que sucede con los contratos de servicios de computación en la nube, suelen ser muy amplias tanto en su ámbito territorial y temporal (ámbito territorial mundial, por tiempo indefinido o por el máximo que permita la legislación sobre propiedad intelectual aplicable al contrato) como por los derechos de explotación que se conceden (derecho de transformación, comunicación pública, distribución, etc.) Las finalidades de estas cesiones no siempre aparecen delimitadas en las condiciones predisuestas por el proveedor, ni siempre se permite al usuario oponerse a ellas.

Por otra parte, el proveedor de la plataforma suele exonerarse de responder por contenidos sujetos a derechos de propiedad intelectual de terceros publicados por los usuarios⁸³.

5.1.3.- Limitaciones y exclusiones de responsabilidad

Al igual que sucede con los contratos de computación en la nube, en los contratos de plataformas de comparación de ofertas turísticas el proveedor realiza

consulta: 22 de marzo de 2017].

83 Las condiciones de la plataforma *Minube* establecen que "en caso de que el usuario integre obras de terceros, o su imagen personal, declara que cuenta con las autorizaciones correspondientes, debiendo asumir de forma exclusiva las responsabilidades que se deriven de posibles reclamaciones. La cesión antes señalada es independiente de si efectivamente se recibió contraprestación. La baja del usuario no afecta en modo alguno los términos de la cesión, por lo que si ésta ocurre, los contenidos aportados no serán retirados", y se exime de responsabilidad "Por eventuales reclamaciones de terceros por concepto de derechos de propiedad intelectual y/o patentes o marcas, en relación con cualquier tipo de contenidos que los usuarios suban al sitio *Minube*. Este tipo de reclamaciones será directamente derivada al usuario, el que responderá en forma íntegra por los daños, perjuicios y gastos jurídicos que se ocasionen". *TripAdvisor*, por su parte, advierte al usuario: "Tenga en cuenta que al enviar contenido al presente sitio web por correo electrónico, mediante publicaciones en el presente sitio web o de cualquier otro modo, incluidos todo tipo de comentarios, opiniones de hoteles, preguntas, sugerencias, fotografías o vídeos, ideas o similares que se incorporen en cualquier envío (...), usted otorga a *TripAdvisor* y a sus empresas afiliadas un derecho no exclusivo, sin regalías, perpetuo, transferible, irrevocable y con pleno derecho de sublicencia para (a) utilizar, reproducir, modificar, adaptar, traducir, distribuir, publicar, crear trabajos derivados, mostrar públicamente y realizar tales envíos en todo el mundo y en cualquier medio, ya sea conocido ahora o concebido a partir de este momento, para cualquier propósito; y (b) utilizar el nombre que envíe en relación con dicho envío". En nuestra opinión, esta licencia de derechos en favor de *TripAdvisor* resulta desproporcionada y desequilibrada, teniendo en cuenta la relación jurídica que vincula a plataforma y usuario. IP [Fecha de consulta: 23 de marzo de 2017].

CAPÍTULO OCTAVO

ciertas exclusiones de responsabilidad. Entre estas exoneraciones, las más comunes son aquellas relacionadas con problemas de disponibilidad, fallos o errores de la plataforma o del software o hardware que la sustenta, con perturbaciones provocadas por terceros, con conflictos entre usuarios de la plataforma a causa de los contenidos publicados, por el contenidos de las opiniones de los usuarios o por el borrado incidental de contenidos, entre otras.

A diferencia de lo que sucede en la prestación de servicios de computación en la nube, en la que existe una relación entre prestador y cliente, deberemos averiguar el servicio que presta efectivamente el operador de la plataforma Web 2.0. Así, en algunas ocasiones, este operador actúa como mediador entre el empresario turístico y su potencial clientela, posibilitando que el internauta tenga conocimiento de ofertas y pueda ponerse en contacto con el proveedor turístico para contratar los servicios. Por ello, es razonable que en estos casos el proveedor se exonere de las eventualidades que puedan surgir en la relación jurídica que nazca entre el empresario turístico y el usuario de la plataforma cuando se formalice el contrato entre ambos⁸⁴.

Sin embargo, existen plataformas que permiten al internauta contratar directamente los servicios turísticos, y cuya actuación es más similar a la de una

84 Como ejemplo, el aviso legal del buscador de servicios y productos *Rastreator.com* aclara en términos sencillos en qué consiste la actividad que presta a los usuarios de su Web 2.0, y distingue su actividad de intermediación de la actividad empresarial de las empresas cuyos precios, opiniones y servicios se comparan: "El usuario, cuando accede a obtener una comparativa de precios o tarifas de productos y servicios ofrecidos por *Rastreator.com*, debe recordar que *Rastreator.com* actúa como simple intermediario independiente a través del proveedor del servicio o producto ofertado en la website de *Rastreator.com*. La función de *Rastreator.com* se limita a ofrecer la comparativa de precios o tarifas del producto o servicio que solicite el usuario y que resulte de los datos suministrados por el usuario a través del cuestionario de *Rastreator.com*, (...) En esos supuestos, el usuario podrá averiguar fácilmente quién es ese proveedor, dado que la información contenida en esa website irá acompañada de un "powered by" seguido del nombre comercial del proveedor (...). No obstante, en estos casos el proveedor se identificará al comienzo de esas comunicaciones comerciales con su nombre comercial, facilitará sus datos de contacto, al igual que hará referencia a cualquier otro dato que resulte obligatorio por Ley. (...). *Rastreator.com* advierte a sus usuarios que las descripciones que se hagan de los productos o servicios ofertados en la website de *Rastreator.com* se realizan a los meros efectos informativos, de acuerdo con la información y documentación que proporcionen a *Rastreator.com* los proveedores de esos productos o servicios". Al quedar fuera de la relación jurídica entre proveedor y cliente, el comparador intermediario también se exime de responsabilidades derivadas del contrato entre aquellos: "El usuario no contrata ningún servicio o producto con *Rastreator.com*, por lo que *Rastreator.com* no será responsable de las condiciones y términos de los contratos que el usuario suscriba con el proveedor correspondiente, tras la comparativa realizada. Asimismo, *Rastreator.com* no es responsable de las posibles contingencias o perjuicios que puedan surgir en la relación entre el usuario y el proveedor durante la vigencia del contrato, e incluso cuando éste haya ya finalizado". [Fecha de consulta: 23 de marzo de 2017].

CAPÍTULO OCTAVO

agencia *online* de viajes (*Online Travel Agency* u OTA), dado que sus funcionalidades permiten introducir datos del cliente para efectuar una "reserva" del establecimiento a través del propio operador y enviar correos electrónicos como confirmación de la reserva, los cuales sirven a modo de prueba por el consumidor a la hora de efectuar el *check-in* en el establecimiento, o su mediación en cancelaciones de reservas. En la práctica, algunos de estos operadores manifiestan asimismo realizar únicamente actividades de intermediación, y se exoneran de cualquier responsabilidad, con lo cual no siempre aparecerá claramente delimitada contractualmente la posición del operador de la plataforma, ya que a menudo manifiesta su ajenidad a la relación entre internauta y empresario turístico. Por ello, consideramos que debe atenderse a la verdadera actividad realizada por la plataforma, (intermediación o comercialización) y no a la que afirma realizar, recogida en los acuerdos que ella misma predispone, especialmente en lo relativo a valorar la validez de la exoneración y limitación de sus responsabilidades⁸⁵.

85 La sentencia del Juzgado de lo Mercantil núm. 3 de Asturias, de fecha 30 de abril de 2012, determinó que la actuación del comparador *Booking* en su relación con el usuario que utilizaba estala plataforma para efectuar una reserva en un establecimiento hotelero iba más allá de la actuación de un mero intermediario, en su fundamento tercero, que "A juicio de este juzgador la intervención de la mercantil demandada va más allá que la mera intermediación, puesto que, en primer lugar, si su actuación se limitara a mediar entre el prestador del servicio (hotel) y el consumidor, su influencia concluiría facilitando los "links" o datos necesarios para identificar los establecimientos hoteleros, siendo absolutamente impropio o innecesario exigir que el consumidor contrate (léase "realice la reserva") a través de su propia página web) y, sobre todo, que la demandada le remita un correo electrónico de confirmación de una reserva "ajena"; (...), también carece de lógica que se registre una reserva por *Booking.com*, con toda la información detallada de la misma, dado que, si se trata de un tercero ajeno a la relación contractual, debería ser la prestadora del servicio hotelero quien realizara la reserva y remitiera un correo electrónico confirmatorio de la misma. (...) Otro dato significativo es el grado de intervención que tiene *Booking.com* en la cancelación de la reserva. (...) Parece evidente que la reserva la efectuó la compañía demandada, así como también gestionó su cancelación, y lo hizo conforme a las condiciones pactadas con su cliente (el actor). La nula intervención (aparición) del hotel en las necesarias e imprescindibles gestiones de reserva y cancelación, obligan a concluir que el vínculo jurídico surgió entre el consumidor (actor) y el prestador de servicios de reservas *online* de hoteles (demandada).(...) Finalmente, la propia relación existente entre *Booking.com* y los hoteles contempla situaciones como la presente, en la que la reclamación la realiza el cliente (consumidor) frente a la demandada. Así, en el documento 3 de los aportados junto con la contestación se incluye expresamente "la obligación que tiene en hotel de indemnizar, compensar y eximir a *Booking.com* de responsabilidades por deudas, costas, casos (incluyendo tarifas y gastos de abogados), daños, pérdidas, obligaciones, demandas de todo tipo, intereses, multas y procesos, que *Booking.com* haya pagado en los siguientes casos: (i) reclamaciones de los clientes relativas a información incorrecta, errónea o engañosa del Hotel en la Página Web (cláusula 6.2 de las condiciones de entrega de *Booking.com* con los establecimientos hoteleros)". Esta cláusula del contrato tipo permite apoyar la anterior conclusión: la parte contratante es *Booking.com*, por más que la prestadora del servicio sea un tercero ajeno (el hotel), sin perjuicio de las eventuales acciones de repetición contractual que la demandada pueda tener frente al prestador del servicio de alojamiento". Así, se declara en esta sentencia la nulidad de las cláusulas del comparador *Booking.com* por exclusión de responsabilidad cuando realmente se entiende que es parte

CAPÍTULO OCTAVO

Por otra parte, las plataformas Web 2.0 que proporcionan datos al internauta sobre servicios proporcionados por terceros empresarios turísticos tampoco suelen responsabilizarse por las inexactitudes en esa información, generalmente facilitada por los propios empresarios turísticos, y que generalmente versa sobre precios o disponibilidad. A nuestro parecer, estas cláusulas son razonables, siempre y cuando no eximan a la plataforma de su propio deber de diligencia, y cuando sus funciones se restrinjan a las de un simple intermediario⁸⁶.

Lo anterior no evita que las Webs 2.0 tengan como parte de su deber de diligencia la adopción de medidas de seguridad que garanticen la seguridad de los datos alojados en sus sistemas y la continuidad de la prestación, si bien, como sucede en la computación en la nube, las garantías que puedan ofrecerse en relación a la seguridad no sean totales⁸⁷.

contractual y no una simple intermediaria: "la demandada deberá de responder de cualquier falta de información, información inexacta, en relación con los servicios prestados o productos ofertados por el hotel, por ser este el objeto principal del contrato de reserva de hotel por ella gestionado, sin que pueda oponer frente al demandante la existencia de estas cláusulas generales por su carácter abusivo. Como anticipamos, es la demandada la que entablaba una relación contractual con el consumidor por medio de la reserva, y se vincula con ella garantizando que los servicios contratados se ajustan a los términos en que fueron ofertados en su página web. Por ello, las limitaciones de responsabilidad que deriven de un incumplimiento contractual o cumplimiento defectuoso deben ser consideradas nulas por abusivas, puesto que no resulta equitativo excluir las eventuales acciones indemnizatorias o de responsabilidad contractual que pudieran corresponder a una de las partes contratantes (en este caso al cliente/consumidor), reenviando a éste a una reclamación frente a un tercero (hotel) con el que no ha establecido directamente vínculo contractual". Más información disponible en: <<http://www.antunaabogados.es/documentos/BOOKING.pdf>>. [Fecha de consulta: 23 de mayo de 2017].

86 El comparador *Rastreator.com* recoge esta exoneración de responsabilidad en sus condiciones: "*Rastreator.com* trata de garantizar el mejor precio actualizado del producto o servicio cuya comparativa solicita el usuario. Sin embargo, *Rastreator.com* no será responsable de posibles errores u omisiones en el precio, cuando éste no coincida con el que se oferte en el enlace facilitado desde la website de *Rastreator.com*, que redirecciona directamente a la website del proveedor del producto o servicio elegido, siempre que la causa del error no se deba a circunstancias imputables a *Rastreator.com*". [Fecha de consulta: 23 de marzo de 2017].

87 Como referencia a la obligación de mantener ciertas medidas de seguridad para garantizar la prestación del servicio, sirva de ejemplo la anterior afirmación del comparador *Rastreator.com*: "A pesar de las medidas de seguridad que se adoptan, *Rastreator.com* no garantiza la ausencia de virus u otros elementos que pudieran dañar o alterar el sistema informático del usuario, ni asume *Rastreator.com* responsabilidad alguna derivada de ello". [Fecha de consulta: 23 de marzo de 2017].

5.2- Problemas específicos entre las plataformas Web 2.0 y el pequeño empresario turístico

Para el pequeño empresario turístico, además de lo anterior, se derivan de las plataformas comparadoras de servicios turísticos ciertas cuestiones igualmente problemáticas, de las cuales creemos conveniente destacar las consecuencias negativas de las opiniones o reviews de clientes en el prestigio de la empresa turística y la imposibilidad por parte de una empresa de eliminar cualquier referencia a su establecimiento cuando no tiene ningún vínculo jurídico con la plataforma.

5.2.1.- La reputación corporativa *online*

En las condiciones de plataformas Web 2.0 aceptadas por los usuarios, que tienen como funcionalidad la posibilidad de publicar opiniones o *reviews* sobre establecimientos u otros servicios turísticos de los cuales han podido disfrutar, el usuario generalmente se compromete a proporcionar únicamente datos veraces, exactos y actualizados⁸⁸. Por su parte, los proveedores de estas plataformas suelen incluir en sus términos de servicio exenciones de responsabilidad respecto de la veracidad de las opiniones vertidas por los usuarios⁸⁹. Asimismo, es habitual que estos operadores se reserven el derecho de eliminar contenidos publicados por los usuarios a su entera discreción⁹⁰. Si bien los operadores no se comprometen a ejercer un control exhaustivo sobre todos y cada uno de los contenidos vertidos en su plataforma, es habitual que realicen operaciones de rastreo y filtrado de opiniones cuestionables⁹¹.

88 Como ejemplo, una cláusula de las condiciones de uso de la plataforma *Minube*: "El usuario declara y garantiza la veracidad y exactitud de los datos proporcionados a *Minube* y se compromete a mantenerlos actualizados en todo momento". Además, "Minube se reserva el derecho a poder eliminar sin previo aviso a usuarios registrados que no respondan a los principios de calidad y veracidad exigidos". [Fecha de consulta: 22 de marzo de 2017].

89 *Minube* establece que no se hará responsable "por falta de veracidad o precisión en la información, así como cambios o modificaciones que las líneas aéreas, hoteles o empresas abocadas al alquiler de coches, puedan cometer o realizar. En este sentido, se informa al usuario que *Minube* presta un servicio de intermediación entre el usuario y las empresas asociadas, por lo que cualquier decisión que éstas adopten en relación con disponibilidad, cambios de precios, o días y horarios, pertenece al exclusivo ámbito de su responsabilidad". [Fecha de consulta: 22 de marzo de 2017].

90 *TripAdvisor* "se reserva el derecho de eliminar, a su entera discreción y sin previo aviso, los mensajes de los usuarios y/o el contenido del sitio por cualquier motivo". Disponible en: <https://www.tripadvisor.es/vpages/review_mod_fraud_detect.html>. [Fecha de consulta: 22 de marzo de 2017].

91 *TripAdvisor* reconoce que "no edita ni controla los mensajes de los usuarios que se publican o distribuyen

CAPÍTULO OCTAVO

Respecto de las opiniones fraudulentas, es decir, aquellas vertidas por usuarios que no han sido clientes del servicio sobre el cual opinan, o los intentos de propietarios o empleados de un establecimiento o servicio que pretenden mejorar la reputación de ese u otro establecimiento emitiendo opiniones negativas, o cualesquiera otras opiniones o comentarios que sean engañosos, las plataformas suelen utilizar también diferentes mecanismos para detectarlas⁹². Sin embargo, la plataforma está obligada a retirar los contenidos si conoce su ilicitud, como exige el artículo 16 de la LSSI, con lo cual el pequeño empresario turístico deberá informar de inmediato a la plataforma sobre la falsedad del contenido, aportando el máximo de pruebas que soporten su defensa y demuestren la lesión de sus derechos, para que esta retire los contenidos⁹³. La legislación y la jurisprudencia únicamente consideran responsables al autor de los comentarios, y no a las plataformas Web 2.0 que permiten como funcionalidad la publicación de opiniones⁹⁴.

El pequeño empresario turístico, frente a estas situaciones, puede iniciar

en el presente Sitio web, incluidos las conversaciones de chat, los tabloneros de anuncios y otros foros de comunicación, y no será responsable ni asumirá ninguna obligación sobre dichos mensajes de los usuarios". Sin embargo, afirma utilizar herramientas automáticas y equipos de moderadores que examinan opiniones cuestionables, y permiten a la comunidad de usuarios "denunciar" contenidos inapropiados de otros usuarios que sean susceptibles de infringir las Políticas de Uso Adecuado del servicio y las normas de publicación de opiniones. Así lo afirma la propia plataforma en su información sobre moderación de opiniones. Disponible en: <https://www.tripadvisor.es/vpages/review_mod_fraud_detect.html>. [Fecha de consulta: 22 de marzo de 2017].

- 92 TripAdvisor responde así a la pregunta "¿Cómo detectáis el fraude?": "Por desgracia, no podemos explicarlo con detalle aquí, porque les ofreceríamos a quienes pretendan cometer fraude las instrucciones para burlar a nuestro sistema. Lo que sí podemos decir es que dedicamos mucho tiempo y recursos a asegurar que el contenido de *TripAdvisor* refleje las auténticas experiencias de viajeros auténticos. Disponemos de especialistas en control de calidad que nos aportan mucha y variada experiencia para mejorar nuestros métodos de prevención y nuestro equipo emplea miles de horas al año para garantizar la integridad de los contenidos de *TripAdvisor*. Además, utilizamos herramientas automáticas que nos ayudan a marcar aquellas opiniones cuyo contenido sea cuestionable para revisarlas, y contamos con una apasionada comunidad de millones de viajeros que no le quitan ojo a nuestra página".
- 93 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."
- 94 MARTÍNEZ NADAL, Apol·lònia, ROSSELLÓ RUBERT, Francisca María, "La experiencia del cliente: análisis jurídico de la publicación *online* de comentarios de clientes. En particular, el caso de TripAdvisor", *Actas de las IX Jornadas de Investigación en Turismo*, Sevilla, 2016, págs. 99 a 128.

CAPÍTULO OCTAVO

acciones en defensa del derecho al honor de la empresa⁹⁵ (Ley Orgánica 1/1982 de 5 de mayo, de Protección Civil del Derecho al Honor; Ley Orgánica 2/1984, sobre el derecho de rectificación; Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, y artículos 205 a 216 del Código Penal, con el fin de retirar los contenidos de la Red que perjudiquen su reputación. A pesar de lo anterior, el establecimiento debe igualmente plantearse la idoneidad de ejercer acciones legales a través de la vía judicial, debido a múltiples circunstancias, como la necesidad de aportar pruebas que acrediten los hechos concurridos o su falsedad, la imputabilidad de estos hechos a una persona física (muchas veces las opiniones se dan de manera anónima), la determinación del perjuicio al establecimiento, los largos trámites y plazos que supone un procedimiento judicial, etc.

Por otra parte, los términos de uso de estas plataformas suelen establecer las consecuencias de la detección de estas opiniones engañosas, aunque estas consecuencias serán determinadas a discreción del proveedor⁹⁶. Conscientes de esta problemática, también se han desarrollado iniciativas en el sector turístico para promover prácticas más equitativas, que destacan los puntos clave. Recordemos que su valor jurídico no es vinculante, sino que tiene los efectos de simples recomendaciones⁹⁷.

5.2.2.- La salida de la empresa turística de la plataforma Web 2.0

95 Del cual es titular, como reconoció el Tribunal Constitucional en su Sentencia 139/1995. Al respecto, ver MARTÍNEZ NADAL, Apol·lònia, ROSSELLÓ RUBERT, Francisca María, *La experiència...*, *op. cit.*, pág. 105.

96 Estas son las consecuencias de *TripAdvisor* ante la detección de opiniones fraudulentas: "Se producen varias consecuencias si determinamos que se han enviado opiniones fraudulentas a un establecimiento: El establecimiento puede caer varias páginas en el índice de popularidad de *TripAdvisor*. Los datos de clasificación de los establecimientos se gestionan caso por caso y son de nuestra propiedad. El establecimiento perderá su derecho a participar en los premios Travellers Choice de *TripAdvisor*, en las listas Top 10, en las notas de prensa, etc. Aparecerá un mensaje de penalización, rojo y grande, en la página del perfil del establecimiento, indicando que las opiniones del establecimiento son sospechosas".

97 Destacaremos la aprobación de las directrices "*Benchmarks of Fair Practices in Online Distribution*", por parte de la Asociación Empresarial Europea de Hoteles, Restaurantes y Cafeterías (HOTREC), en las que se dedica un apartado a las opiniones *online* de clientes sobre estas categorías de establecimientos. El apartado 17 destaca las cuestiones más importantes para una valoración justa y equitativa de los servicios prestados por el sector hostelero, como la falta de control editorial, la falta de herramientas que detecten opiniones manipuladas, la posibilidad de un derecho de réplica, etc. HOTREC, "*Benchmarks of Fair Practices in Online Distribution*" [en línea]. Disponibles en: <<http://www.hotrec.eu>>. [Fecha de consulta: 23 de marzo de 2017]. Ver también MARTÍNEZ NADAL, Apol·lònia, ROSSELLÓ RUBERT, Francisca María, *La experiència...*, *op. cit.*, pág. 116.

CAPÍTULO OCTAVO

Una de las cuestiones que se plantea el pequeño empresario del sector turístico es cómo salir de una plataforma que aloja opiniones o *reviews*, en la cual nunca se ha dado de alta ni comparte vínculo contractual alguno (incluso, puede ocurrir que esta empresa turística ni siquiera tenga página web propia o perfil público en ninguna red social). En este caso, han sido terceros quienes, al verter sus opiniones sobre el servicio turístico y en uso de las funcionalidades de esa plataforma, involucran al pequeño empresario en la comunidad de usuarios, sin que este, como titular del establecimiento o proveedor del servicio turístico valorado, haya tenido la posibilidad de consentir o negarse.

La eliminación de contenidos de la plataforma queda a discreción del propio proveedor, tal y como suele establecer en sus términos de uso. Ello, no obstante, perjudica al pequeño empresario turístico, al no poder decidir libremente sobre si quiere o no que su establecimiento aparezca en la concreta Web 2.0, independientemente de la existencia o no de opiniones negativas de usuarios sobre la calidad de su servicio o establecimiento.

Los proveedores establecen que, al tratarse de comunidades de usuarios, se busca la obtención de la máxima información sobre la calidad de cualesquiera establecimientos turísticos de esa categoría que oferten servicios en el mercado. Algunos operadores manifiestan que su plataforma también sirve para "denunciar" servicios deficientes o prestados por empresas que han intentado falsear de algún modo su reputación *online*, con lo cual, para que el consumidor turístico esté alertado si decide contratar en este tipo de establecimientos, no solo no les permiten retirar su presencia del sitio web, sino que etiquetan al establecimiento a modo de advertencia⁹⁸.

Si bien estamos a favor de que el consumidor tenga una opinión libre y pueda expresarla y compartirla en comunidad, también consideramos que deben ofrecerse mecanismos de defensa a las empresas perjudicadas por opiniones de usuarios. Debe tenerse en cuenta que la empresa turística, aunque puede ver perjudicada su

98 TripAdvisor responde así a la pregunta "¿Por qué no eliminan directamente de la página web los establecimientos que hayan cometido fraude?", en sus *Preguntas frecuentes sobre moderación de opiniones y detección de fraude*: "Eso es exactamente lo que quieren algunos establecimientos. Nos parece que el mensaje rojo es mejor castigo y ofrece más información a los viajeros para que puedan tomar la mejor elección posible". Disponible en: <https://www.tripadvisor.es/vpages/review_mod_fraud_detect.html>. [Fecha de consulta: 24 de marzo de 2017].

CAPÍTULO OCTAVO

reputación y menguados sus ingresos con ciertas opiniones vertidas en Webs 2.0 que permitan la expresión de opiniones de usuarios, no siempre tiene ocasión de alegar o defenderse. Existen muchas circunstancias que no pueden valorarse con una simple opinión de un cliente, como sucesos ocasionados de manera puntual, mal interpretados, manipulados o falsos, que tuvieron lugar años atrás, que sucedieron bajo las directivas de otros propietarios o gestores, etc.

Además, aunque la plataforma decida atender a la petición de retirar las referencias sobre una empresa o de opiniones sobre esta vertidas por usuarios, generalmente no se establece un procedimiento transparente o rápido para ello, con lo cual la opinión o la empresa sigue estando accesible para el resto de la comunidad de viajeros durante un tiempo, con los consiguientes perjuicios para la reputación y el lucro cesante que ello supone. Tampoco se asegura que, tras finalizar este proceso de retirada de la opinión u opiniones por parte de la plataforma, esta comunique a la comunidad de internautas tal rectificación, o muestre un mensaje que permita limpiar la reputación dañada de la empresa que no lo merecía, a modo de "opinión falsa", "incidencia solventada", "cambio en la directiva", etc.

Para solventar estas cuestiones, proponemos al legislador una regulación similar al "derecho al olvido" que tenga como destinatarias a las personas jurídicas, y especialmente al pequeño empresario turístico, para que pueda decidir libremente sobre si quiere o no pertenecer a este tipo de plataformas y para que pueda defenderse de potenciales abusos, y no quede desamparado ante actuaciones arbitrarias de clientes u operadores de Webs 2.0. Asimismo, sería recomendable sancionar ciertas prácticas comerciales engañosas, como la publicación de opiniones falsas o manipuladas sobre establecimientos que se promocionan a través de plataformas de opinión, las vierta el propio establecimiento, otro establecimiento de la competencia o un usuario. No obstante, debería igualmente ponderarse este derecho del empresario a retirar su presencia de ciertas plataformas con otros derechos de terceros, como puede ser el derecho a la libertad de expresión del usuario y a la libertad de información.

CAPÍTULO OCTAVO

6.- CONCLUSIONES Y RECOMENDACIONES AL PEQUEÑO EMPRESARIO DEL SECTOR TURÍSTICO SUScriptor DE SERVICIOS *CLOUD*

En nuestra opinión, en cuanto a la migración de datos por parte del pequeño empresario del sector turístico a sistemas de computación en la nube, se tendrá en cuenta:

1.- La solvencia y garantías que ofrece el proveedor *cloud*, especialmente respecto de la calidad y continuidad del servicio, de la legislación aplicable al contrato y del cumplimiento de las obligaciones en materia de protección de datos, debiendo priorizarse lo anterior frente a otros aspectos como su popularidad o su precio. Es relevante tener constancia de los países en los cuales se pueden almacenar o replicar los datos migrados.

2.- La naturaleza de los datos y su sensibilidad, sean datos personales o de contenido empresarial, con el fin de sopesar los riesgos de su migración

3.- Adecuar siempre el tratamiento de datos personales a la finalidad por la cual fueron recabados, y asegurar el cumplimiento íntegro de la normativa sobre privacidad. En particular, consideramos oportuno revisar los formularios de recolección de datos para incorporar la petición del consentimiento que permita transferirlos a proveedores *cloud*, especialmente cuando sea aplicable el nuevo Reglamento General de Protección de Datos, con el fin de informar y recabar el consentimiento del titular de datos personales que se traten a través de servicios *cloud* que impliquen transferencias internacionales de datos.

4.- Revisar eventuales limitaciones o exclusiones de responsabilidad que pueda efectuar el proveedor *cloud*.

5.- Averiguar el destino de los datos migrados una vez finalizada la relación de servicios, y la posibilidad de recuperarlos con el fin de reutilizarlos, ya sea en integrándolos en sistemas informáticos de la empresa o transmitiéndolos a sistemas de otro proveedor *cloud*.

Para finalizar, creemos que los pequeños empresarios turísticos pueden sacar mucho provecho de la computación en la nube, tanto en ahorro de costes como en

CAPÍTULO OCTAVO

optimización de la actividad empresarial. Sin embargo, deben conocerse los retos jurídicos que se le presentan, puesto que la normativa vigente no siempre tiene en cuenta las particularidades del sector. A la espera de modificaciones legislativas que doten de mayor protección y seguridad jurídica al pequeño empresario, pertenezca o no al sector turístico, el principio de buena fe y unas condiciones contractuales transparentes son la mejor garantía para la exitosa implementación de servicios de computación en la nube y la mejora de la confianza entre el proveedor de servicios *cloud* y el pequeño empresario suscriptor.

CONCLUSIONES

CONCLUSIONES

Para finalizar este trabajo, a continuación recopilaremos las principales conclusiones que se derivan de este estudio relativo a los contratos de computación en la nube pública para pequeños empresarios.

PRIMERA. Generalidades. Es evidente que el ritmo de la actividad normativa difícilmente se adaptará a la vertiginosa velocidad con la cual se desarrolla la tecnología. El impacto de la computación en la nube sobre la realidad económica y jurídica y su uso masificado obligan a reinterpretar la normativa existente y a adaptarla a nuevos supuestos de hecho inicialmente no previstos por el legislador. Ante nosotros se presenta el reto de combinar el marco legal nacional y comunitario aplicable, que incluye normativa sumamente variada (propiedad intelectual y secreto profesional, normas sobre obligaciones y responsabilidades contractuales, legislación sobre servicios de la sociedad de la información y sobre protección de datos, etc.), con las especificaciones técnicas del concreto servicio de computación en la nube pública suscrito (infraestructura, plataforma y software), y con las prácticas contractuales que el suscriptor no puede negociar.

SEGUNDA. Elementos subjetivos del contrato. Contrato bajo condiciones generales. A diferencia de lo que suele pensarse, el consumidor no es única parte vulnerable de la contratación de servicios de computación en la nube, sino también el pequeño profesional o empresario que contrata estos servicios sin pleno conocimiento de sus implicaciones. Este último puede ver afectados su reputación, su información empresarial, su patrimonio y su continuidad como empresa (al no tener acceso a sus datos). Consideramos necesario un mayor amparo jurídico para este colectivo, especialmente aquellos cuya actividad profesional está desvinculada de técnicas y conocimientos informáticos.

CONCLUSIONES

Por este motivo hemos propuesto la aplicación extensiva del control de contenido de las condiciones generales a este colectivo. Como contrapartida, resulta primordial, a nuestro parecer, la confianza que brinda el proveedor de servicios al suscriptor, fundamentada en la información que le ofrece sobre el contenido del servicio y los detalles de la transacción, todo ello en términos fácilmente comprensibles para este, con el fin de que entienda su funcionalidad y sea consciente de las obligaciones que asume al contratar. A fin de cuentas, una actuación informada, transparente y honesta no puede sino revertir en beneficio del propio proveedor: su actividad comercial será más rentable y segura, y a su vez le facilitará la limitación y exclusión de responsabilidades que no le corresponden ante consumidores y terceros.

TERCERA. Definición técnica y jurídica de *Cloud Computing*. Aunque el término "computación en la nube" o "*Cloud Computing*" resulta ampliamente utilizado, y la definición adoptada por el NIST se ha consolidado en el sector como concepto de referencia, la delimitación técnica de todos los servicios que abarca la computación en la nube pública no está exenta de discusión, especialmente en lo referente al software como servicio. Consideramos apropiado adoptar un concepto amplio de computación en la nube pública, incluyendo dentro de este aquellas aplicaciones *cloud* que presentan ciertas características, tales como la necesidad de autenticación del usuario, el almacenamiento remoto de información creada o migrada por el usuario, la posibilidad de que pudiera implementarse su pago por uso, que sea escalable y elástica, que permita ciertas facultades de personalización, que implique la suscripción de condiciones generales o que sean aplicaciones especialmente complejas o potentes. Así, servicios que compartan las anteriores características y que permitan funcionalidades del tipo comunicación social, compartición de información, almacenamiento de contenidos o edición colaborativa de archivos son, en nuestra opinión, softwares como servicio que se implementan en la modalidad de nube pública.

Algunas instituciones como la Comisión Europea, el Grupo de Trabajo del Artículo 29, la Agencia Española de Protección de Datos o la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) han descrito el *Cloud Computing* para proceder posteriormente al tratamiento de algunos de sus aspectos jurídicos, si bien las definiciones adoptadas toman igualmente como referencia las capacidades y funcionalidades prestadas al suscriptor, estableciendo un concepto no uniforme pero sí similar de los servicios que comprenden la

CONCLUSIONES

computación en la nube.

CUARTA. Naturaleza, características y noción del contrato de computación en la nube pública. El contrato de *Cloud Computing* de implementación pública resulta ser un contrato atípico. Asimismo, al no identificarse con una única prestación sino con múltiples, aunque coincide con la esencia del genérico contrato de servicios resulta un contrato complejo, al compartir obligaciones pertenecientes a otras figuras jurídicas tipificadas como el depósito o el suministro, y obligaciones coincidentes con las de otras figuras habituales en el tráfico mercantil (suministro mercantil, *Hosting*, licencias de uso no personalizado de software, etc.). El contrato de computación en la nube pública debe distinguirse asimismo de los contratos de *Outsourcing* informático y *Hosting*, pues si bien pueden parecer similares, difieren tanto en el objeto contractual y en la formación del contrato como en las concretas obligaciones asumidas por las partes contratantes.

El contrato de computación en la nube es un contrato consensual, bilateral, sinalagmático, oneroso (aunque no necesariamente dinerario), de tracto sucesivo y prestado a través de medios electrónicos, concretamente mediante redes de comunicaciones. Cabe añadir que este trabajo se centra en contratos suscritos por empresarios, con lo cual afirmamos su carácter mercantil, si bien, a diferencia del *Outsourcing*, esta característica no se presenta como esencial del servicio, sino que este se presta tanto a clientes consumidores como profesionales.

Definimos el contrato de computación en la nube de implementación 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.

Aunque pueden existir diferencias derivadas de los distintos modelos de servicios de nube pública (infraestructura, plataforma o software) en los contratos,

CONCLUSIONES

dependiendo de las concretas capacidades o funcionalidades contratadas, pudiendo implicar una diferente distribución en las tareas de gestión de los recursos y la distinción entre los deberes de diligencia de prestador y suscriptor, las obligaciones propias del contrato de computación en la nube pública serán coincidentes. Asimismo, los acuerdos de nivel de servicio, que recogen los compromisos del proveedor relacionados con la parte técnica de la prestación del servicio y objetivizan su deber de diligencia profesional, pueden diferir de un contrato a otro. Para minimizar tales diferencias, es recomendable que los proveedores se adecuen a los estándares existentes al respecto, especialmente ahora que la Comisión Europea ha publicado trabajos respecto de la homogeneización de estándares en servicios de *Cloud Computing*.

QUINTA. Obligaciones de las partes. Las obligaciones de un proveedor de nube pública se pueden dividir en tres acciones complementarias. En primer lugar, la conectividad y disponibilidad del servicio y de los recursos computacionales, lo cual implica un adecuado diseño y mantenimiento de los equipos físicos y de los elementos de software que permiten al cliente el uso eficiente del servicio.

En segundo lugar, la obligación de suministrar las capacidades al suscriptor de manera elástica (y hasta el límite contratado, si lo hubiera), fiable y sencilla, y cuando impliquen una capacidad de almacenamiento de datos, a la custodia de estos de manera íntegra y confidencial, y a facilitar al suscriptor su recuperación. Respecto de los datos migrados, el proveedor poseerá un mayor control y responsabilidad por los datos en los servicios de software, que irá decreciendo en los servicios de plataforma, y que será aún menor en los servicios de infraestructura. Ello es así debido al diferente grado de control y gestión de la seguridad que ofrecen al cliente cada una de las diferentes modalidades de servicios *cloud*. Creemos que la preservación de la integridad de los datos debería alcanzar el momento en el cual los datos se devuelven al cliente una vez extinguida la relación contractual, o se transmiten a otro proveedor, puesto que hasta ese momento persiste en el proveedor el deber de diligencia como prestador del servicio *cloud* contratado, y a su vez se genera en el cliente una expectativa legítima de recuperar los datos que ha alojado en los sistemas remotos de aquel. Por otra parte, los contratos generalmente no extienden la obligación del proveedor de mantener la confidencialidad de los datos una vez extinguido del contrato. Sería recomendable, bajo nuestro punto de vista, que se prolongase este deber, como mínimo, hasta el momento en que se haya hecho efectivo el borrado de los datos una vez facilitada la portabilidad de estos a otro

CONCLUSIONES

proveedor o su recuperación por el cliente, especialmente si se trata de datos de carácter personal o con potencial valor comercial.

En cuanto a los aspectos técnicos, el contrato quedará sujeto a los objetivos del nivel de servicio establecidos al respecto en el acuerdo de nivel de servicio, y, en su defecto, a un abstracto deber de diligencia profesional del proveedor de servicios de computación en la nube, debiéndose tomar como referencia a tal efecto, y a falta de regulación específica, los usos del sector.

En tercer lugar, la obligación de facilitar información transparente antes y durante el transcurso de la prestación, con el fin de que el suscriptor pueda valorar la utilidad del servicio y el cumplimiento de las obligaciones legales en materia de protección de datos, los costes y otras cargas que supone la suscripción del servicio (sean o no dinerarios) y de los efectos derivados de la extinción del contrato, como la recuperación de los datos o su borrado. El proveedor debe prestar el servicio conforme a la información precontractual facilitada al cliente (art. 1258 Código Civil).

El proveedor *cloud* pertenece asimismo a la categoría de prestadores de servicios de la sociedad de la información de acuerdo con la LSSI, y presta actividades de intermediación, con lo cual estará sujeto a las obligaciones que la LSSI impone a esta figura jurídica cuando tal ley le sea de aplicación.

A nuestro parecer, si bien la asunción de responsabilidad del proveedor debe ser proporcional a la contraprestación del cliente, y no consideramos equiparables las exigencias de un contrato de pago a las de un contrato sin contraprestación dineraria (dado que el primero debería implicar un mayor compromiso por parte del proveedor que el segundo), no se puede obviar la cobertura de expectativas mínimas que el cliente legítimamente espera al suscribir un contrato de *Cloud Computing*, ya que estas derivan de la propia naturaleza jurídica de ese contrato, aunque no se remunere monetariamente.

Las obligaciones del suscriptor son el pago del precio o la asunción de las cargas asociadas al servicio, el deber de colaboración con el proveedor y el uso del servicio de acuerdo con lo acordado en la política de uso adecuado (PUA). Asimismo, será recomendable que el cliente profesional suscriptor de servicios *cloud*, en su propio beneficio, informe al proveedor sobre sus necesidades particulares y expectativas, con el fin de que el servicio se adecue al máximo a sus particulares necesidades, ya que el proveedor no está obligado a prestar un servicio

CONCLUSIONES

específicamente adaptado a las concretas necesidades concretas de cada cliente suscriptor, sino que los servicios se ofertan de manera estandarizada. El propio deber de diligencia profesional del pequeño empresario exigirá una valoración previa de las ventajas y riesgos antes contratar y migrar sus datos a los sistemas de un determinado proveedor de servicios de computación en la nube.

SEXTA. Responsabilidades. Cumplimiento defectuoso. La responsabilidad del proveedor *cloud* debido a incidentes de seguridad dependerá de la efectiva implementación de las medidas de seguridad del servicio, de cuán previsible y evitable haya sido la contingencia, y de las limitaciones y exclusiones de responsabilidad que el cliente pequeño empresario haya aceptado a través de las cláusulas contractuales. Respecto de estas últimas, proponemos que se valore su potencial abusividad en aquellos casos en los cuales la situación de indefensión del pequeño empresario sea equiparable a la de un consumidor.

Cuando se produzcan alteraciones en el servicio o daños que tengan su origen en actuaciones de subproveedores *cloud*, el proveedor principal responderá por reclamaciones ante el cliente (art. 1903 Código Civil), sin perjuicio del derecho de repetición del proveedor (art. 1904 Código Civil). Además de lo anterior, consideramos que, en aquel caso en que el subproveedor no haya instaurado en sus sistemas medidas de seguridad mínimas que garanticen al proveedor principal la prestación del servicio en las condiciones que oferta al cliente o usuario final, puede existir culpa *in eligendo* del proveedor al seleccionar al subproveedor, teniendo en cuenta la habitual mediación de un acuerdo de nivel de servicio entre ambos.

Los objetivos de nivel de servicio concretan unos niveles mínimos de calidad del servicio, y no alcanzar esos objetivos no implica la resolución del contrato, sino que esta únicamente tendrá lugar en casos de incumplimiento especialmente grave o que implique la manifiesta ineficiencia del servicio contratado. No obstante, sí sirven como referencias para determinar eventuales cumplimientos defectuosos. La falta de consecución de algunos de estos objetivos no implica una compensación total de los daños sufridos por el usuario, debido a la común inclusión en el contrato de los denominados *service credits* o "créditos de servicio". Estas "compensaciones" permiten al cliente una rebaja en futuras facturaciones al no alcanzarse los mínimos acordados como objetivos de nivel de servicio, pero debido a su escaso importe y a ciertas condiciones a las cuales se vincula su concesión, no funcionan como verdaderos mecanismos de resarcimiento ni de penalización. Si bien permiten ajustar

CONCLUSIONES

el precio del servicio ante prestaciones defectuosas, con lo cual pueden resultar útiles cuando el incumplimiento defectuoso resulta meramente ocasional, también es cierto que obstaculizan, por una parte, la resolución del contrato ante incumplimientos defectuosos que se repitan durante la ejecución del servicio (pues obligan a la permanencia en el servicio para obtener su disfrute), y, por otra parte, la reclamación de otras indemnizaciones por los daños y perjuicios efectivamente ocasionados. Por ello, consideramos que los tribunales pueden valorar su admisibilidad.

Asumir el servicio tal y como se presta implica para el pequeño empresario la renuncia a las garantías que le correspondan por daños directos (daños a equipos o dispositivos, al software instalado, a datos, etc.) y por pérdidas que pueda sufrir debido a un funcionamiento deficiente del servicio *cloud* contratado. Consideramos que estas prácticas, las cuales podemos calificar como abusivas, se van consolidando en el sector, quedando el adherente pequeño empresario en una eventual posición de desamparo.

SÉPTIMA. Legalidad de los contenidos y responsabilidades de cliente y proveedor al respecto. Política de uso adecuado (PUA). En los contratos de computación en la nube, el suscriptor asumirá la responsabilidad por los contenidos que el mismo alojada en los sistemas del proveedor, mediante los compromisos que forman parte de las políticas de uso adecuado del servicio *cloud*. En estas políticas se establecen los usos permitidos y prohibidos del servicio. No obstante lo anterior, el proveedor tiene ciertas responsabilidades derivadas de su categorización como prestador de servicios de intermediación por la LSSI. Si bien no se le exige la supervisión de los contenidos de los usuarios, si se considera que ha tenido conocimiento efectivo de datos ilícitos alojados en sus sistemas y que están accesibles a terceros, deberá proceder de manera diligente a bloquear el acceso a tales contenidos y/o proceder a su retirada, (art. 16 LSSI). En caso contrario, podría ser considerado responsable por tales contenidos alojados. A su discreción, el proveedor podrá realizar monitorizaciones para comprobar el cumplimiento de las PUA por parte de los usuarios, y valorar sobre la suspensión del servicio al usuario infractor. A su discreción, el proveedor podrá realizar monitorizaciones para comprobar el cumplimiento de las PUA por parte de los usuarios, y valorar sobre la suspensión del servicio al usuario infractor. También estará obligado a colaborar con las autoridades competentes cuando así se lo requieran (art. 11 LSSI).

CONCLUSIONES

Los contenidos de proveedor y suscriptor involucrados en la prestación del servicio se protegerán jurídicamente de acuerdo a su naturaleza, (obras sujetas a derechos de autor, secretos empresariales, propiedad industrial), debiendo atenderse, por una parte, a lo establecido al respecto por la normativa específica que pudiera ser aplicable y, por otra, a las licencias de uso concedidas por el titular a la contraparte o a terceros.

La información creada por el proveedor a través de monitorizaciones, metadatos, *cookies* o sistemas de analítica a partir de actividades o datos introducidos por el suscriptor podría resultar protegida por el deber de confidencialidad, al tratarse de una de las obligaciones inherentes al contrato de computación en la nube, puesto que quedarán fuera de la protección legal de la propiedad intelectual o los secretos empresariales. Habitualmente, estos datos no suelen tener valor aisladamente considerados, sino en los patrones derivados del análisis del comportamiento en la comunidad de usuarios del servicio *cloud*. A no ser que pueda demostrarse que el proveedor o el tercero que explota tales datos provoca perjuicios al usuario u obtiene considerables beneficios económicos que el usuario dejaría de percibir de igual forma si hubiese gestionado esa información por su propia cuenta, no existirá posibilidad de reclamación económica.

Asimismo, los datos de carácter personal se protegerán jurídicamente atendiendo a su normativa específica.

OCTAVA. Contratos de computación en la nube pública y protección de datos de carácter personal. Portabilidad de datos personales. La protección de datos personales se configura como uno de los apartados más relevantes dentro de la contratación de servicios de computación en la nube. Ello es así porque, además de la relación mercantil existente entre proveedor *cloud* y pequeño empresario, se crea otra relación jurídica derivada de la normativa en materia de protección de datos: la relación entre el pequeño empresario responsable del tratamiento y el proveedor *cloud* encargado del tratamiento, utilizando el primero los servicios del segundo para efectuar tratamientos automatizados de datos personales de terceros.

Si bien el pequeño empresario responsable del tratamiento debe recabar el consentimiento informado del titular de los datos personales para poder tratarlos, no está obligado, de acuerdo con la actual LOPD, a comunicarle específicamente que todo o parte de ese tratamiento podrá efectuarse mediante servicios *cloud*, aunque lo anterior suponga una transferencia internacional de datos. No obstante, con el nuevo

CONCLUSIONES

Reglamento europeo, cuando el servicio *cloud* contratado implique que parte de ese tratamiento de datos del titular se llevará a cabo en sistemas remotos ubicados fuera de las fronteras europeas, el pequeño empresario responsable deberá informar al titular de esos datos personales de la eventual transferencia de datos a terceros países y de sus garantías legales, y obtener su consentimiento inequívoco y expreso al respecto.

Tras la anulación de los principios *Safe Harbor* y la posterior suscripción del Acuerdo *Shield* o Escudo de Privacidad entre la Comisión Europea y EE. UU., los proveedores *cloud* norteamericanos adscritos a este acuerdo se convierten en importadores con un nivel adecuado de protección, al igual que aquellos proveedores radicados en el Espacio Económico Europeo o en otros países que han recibido la aprobación de la Comisión Europea, y por ello se entiende que presentan las suficientes garantías legales. Las transferencias internacionales de datos personales a proveedores *cloud* establecidos en países sin un nivel adecuado de protección según la Unión Europea presentarán las suficientes garantías legales cuando se suscriban entre exportador e importador de datos las cláusulas tipo aprobadas por la Comisión Europea o, en su defecto, las cláusulas tipo aprobadas por una autoridad en materia de protección de datos (AEPD, Grupo de Trabajo del Artículo 29, etc.) que le otorgue seguridad jurídica.

Por otra parte, en la práctica, el proveedor *cloud* poseerá ciertas facultades sobre la información de carácter personal migrada por el pequeño empresario, las cuales pueden colisionar con su papel de mero encargado del tratamiento. Ello es así porque, primeramente, esa información se aloja en sus equipos (o en equipos de sus subproveedores). En segundo lugar, porque es el proveedor *cloud* quien predispone las cláusulas contractuales y, con ellas la política de privacidad y la decisión sobre ciertas finalidades y usos de esos datos. El pequeño empresario tiene la obligación de escoger un proveedor *cloud* que le ofrezca las máximas garantías de cumplimiento legal. No obstante, cuando la política de privacidad exceda de la mera determinación de cuestiones técnicas y organizativas delegables de responsable a encargado, y el proveedor decida unilateralmente sobre cuestiones que afecten a la legitimidad del tratamiento de datos personales de terceros (finalidades, consentimiento necesario, duración de la conservación, acceso, etc.), este proveedor *cloud* será considerado responsable del tratamiento respecto de tales decisiones, puesto que son competencia del rol legal del responsable, de acuerdo con su capacidad de decisión sobre el tratamiento. Lo mismo sucederá cuando no cumpla con las instrucciones del

CONCLUSIONES

responsable o incumpla el acuerdo sobre ambos referente al tratamiento.

El proveedor *cloud* también será responsable ante el pequeño empresario por los daños y perjuicios ocasionados por sus actuaciones o las de sus subencargados al realizar operaciones de tratamiento, teniendo que responder el pequeño empresario responsable ante el titular de los datos personales tratados mediante los sistemas *cloud*.

El titular de los datos personales podrá ejercer sus derechos ante el pequeño empresario responsable del tratamiento. Entre estos derechos cabe destacar el próximamente exigible derecho a la portabilidad. A nuestro parecer, este derecho puede desglosarse en dos derechos: el derecho del titular a recuperar los datos personales procesados por el responsable (derecho de recuperación) y el derecho a poder transmitir esos datos a otro responsable sin impedimentos (derecho a la portabilidad en sentido estricto). El formato en el cual deben entregarse debe ser estructurado, de uso común y lectura mecánica, con el máximo de metadatos posibles, permitiendo la interoperabilidad. Este derecho operará en cualquier momento durante la relación entre responsable e interesado, extendiéndose hasta el periodo de retención de los datos. Cuando el pequeño empresario no disponga de los conocimientos técnicos o la infraestructura adecuada para garantizar este derecho, podrá exigir, como responsable del tratamiento, que el encargado colabore en la realización de esta tarea, a lo cual el proveedor *cloud* deberá responder como corresponde a su posición jurídica de encargado del tratamiento que actúa bajo las instrucciones del primero. Respecto del derecho a la portabilidad, consideramos necesaria su extensión a datos que no tengan carácter personal, como parte de las obligaciones del proveedor y como consecuencia natural del deber de custodia que se deriva de la propia naturaleza jurídica del contrato.

NOVENA. Modificación, suspensión y extinción del contrato. Recuperación y portabilidad de datos no personales. Preservación y borrado de datos. La naturaleza dinámica del servicio de computación en la nube motiva la existencia de cláusulas que habiliten al proveedor a modificar la prestación del servicio y/o el contenido contractual. Cuando estas novedades impliquen un menoscabo en el servicio o en su percepción por el cliente, es recomendable que las cláusulas relativas a modificaciones unilaterales del contrato se interpreten restrictivamente. Asimismo, debería informarse al cliente de tales cambios, de manera previa cuando ello sea posible, y que se le ofrezca la oportunidad efectiva de terminar el contrato sin

CONCLUSIONES

penalización, de acuerdo con la buena fe contractual y el deber de diligencia del proveedor. Nos parece que debe evitarse la presunción de que el cliente que continúa en el uso del servicio *cloud* conoce y está aceptando los cambios efectuados unilateralmente por el proveedor.

En los casos de suspensión del servicio al cliente, el proveedor aparece como único juzgador que examina y decide sobre la continuidad, con lo cual el cliente puede ver mermada su facultad de alegación y defensa. Recomendamos, en aplicación del principio de buena fe contractual, que el contrato establezca los motivos que puedan implicar la suspensión del servicio a un usuario (impago, incumplimiento de PUA, riesgos para la continuidad o seguridad del servicio, etc.) y que se determinen procedimientos internos que incluyan la notificación previa a la suspensión, la posibilidad de formular alegaciones al suscriptor, un plazo para subsanar la acción que motiva la decisión cuando ello sea posible, y la posibilidad de rescatar la información migrada. Todo ello porque la actividad del cliente pequeño empresario puede verse afectada debido a una súbita detención del suministro de la capacidad informática contratada con el proveedor *cloud*, provocándole perjuicios. Recordemos que la continuidad en la prestación del servicio se configura como una de las obligaciones principales del proveedor *cloud*, con lo cual recomendamos que esta cláusula se interprete de manera restrictiva.

La extinción definitiva del contrato *cloud* puede tener lugar por desestimiento unilateral, por resolución por incumplimiento contractual o por fuerza mayor o caso fortuito. No obstante, y aunque las causas de extinción se relacionan con aspectos relativos a la responsabilidad contractual y a la modificación y suspensión unilaterales del servicio, consideramos que la verdadera relevancia del fin de la relación contractual radica en sus eventuales efectos sobre la información migrada por el cliente. Estos efectos son, por una parte, la recuperación por el cliente y, en su caso, la portabilidad de los datos migrados, y, por otra, la retención y borrado de los datos remanentes en los sistemas del proveedor. Ambas cuestiones (portabilidad y borrado) integran lo que se entiende como "reversibilidad del servicio de computación en la nube".

La expectativa del cliente de recuperar los datos trae causa en el propio objeto del contrato, aunque en ciertos casos puede dudarse de si el proveedor está habilitado a no facilitar su devolución. Consideramos que la falta de pago no exime al proveedor de la obligación de permitir recuperar al cliente sus contenidos si

CONCLUSIONES

finalmente se extingue la relación jurídica (aunque puede haberle negado el acceso a sus contenidos o a la funcionalidades del servicio de manera temporal debido a ese incumplimiento), sin perjuicio de que posteriormente reclame al cliente los importes devengados a través de los cauces legales habituales y decida rescindir el contrato. Cuando el proveedor decida extinguir el contrato ante una presunta violación de la política de uso adecuado, para que proveedor retenga los datos del cliente debe tratarse de una inobservancia suficientemente grave, o que con la restitución puedan perjudicarse otros intereses merecedores de ser igualmente protegidos, como por ejemplo, derechos de propiedad intelectual de terceros, la utilización segura del servicio por parte de otros usuarios, etc.

La portabilidad se relaciona con el formato de retorno de los contenidos. De este modo, cuando estos contenidos migrados por el cliente (sean aplicaciones software u otro tipo de datos) puedan transportarse con facilidad a otro sistema *cloud* sin tener que volver a teclearlos, reescribirlos o reprogramarlos, podremos hablar de portabilidad de contenidos. Es recomendable el uso de formatos abiertos o estandarizados para facilitar la portabilidad.

Las previsiones contractuales en relación a la portabilidad son útiles, aunque heterogéneas: en ellas encontramos proveedores que garantizan la portabilidad de los contenidos y otros proveedores que no la garantizan (por ejemplo, que mencionan realizar "esfuerzos comercialmente razonables"), e incluso contratos que no hacen referencia a la portabilidad. Puesto que no puede hablarse de la portabilidad de datos no personales como un derecho, cabe que el proveedor la configure como un servicio añadido en cuyo caso deberá tener un coste razonable que no signifique para el cliente la permanencia en el servicio *cloud*. La portabilidad de datos no personales podrá sustentarse en los deberes de colaboración entre las partes y buena fe contractual.

Cuando la relación contractual entre proveedor y cliente haya llegado a su fin, se mantendrá la obligación del proveedor de custodiar los datos remanentes en sus sistemas que, por ciertas razones, el proveedor esté habilitado a conservar.

El borrado de los datos resulta un aspecto importante en cuanto a la seguridad de los datos migrados, tengan o no carácter personal, puesto que un borrado ineficaz o inexistente puede provocar riesgos e incertezas en cuanto a la confidencialidad e integridad de datos remanentes en sistemas del proveedor. Por contrapartida, un buen acuerdo de confidencialidad puede minimizar los riesgos de un mal proceso de

CONCLUSIONES

borrado, porque la relevancia jurídica del borrado de datos consiste en que los derechos del cliente y de terceros queden salvaguardados, y ello puede compatibilizarse con copias de esos contenidos que se mantengan íntegras y confidenciales. No obstante, este tipo de acuerdo no resulta frecuente en suscripciones de servicios de nube pública bajo condiciones generales de contratación.

El proveedor, de acuerdo con su deber de diligencia, instaurará medidas técnicas que garanticen que los datos remanentes en sus sistemas se mantengan confidenciales. Sin embargo, consideramos que el borrado de los datos no forma parte del obligaciones principales de la naturaleza jurídica del contrato de computación en nube pública, a diferencia de lo que ocurre con el deber de custodia de esos datos, dado que el proveedor *cloud* puede conservarlos por diferentes motivos, siendo uno de ellos la espera hasta que el borrado por sobreescritura los convierta en prácticamente irrecuperables. Lo anterior no impedirá que, ante problemas relacionados con la confidencialidad de estos datos, el proveedor de servicios deba responder incluso tras darse por extinguida la relación contractual entre las partes, como una extensión temporal del deber de custodia, el cual sí forma parte del contenido esencial del contrato de computación en la nube. Asimismo, el borrado de datos personales resultará obligatorio en cumplimiento de la normativa de privacidad.

DÉCIMA. Contratación de servicios de computación en la nube pública por el pequeño empresario turístico. Las diferentes ramas empresariales dedicadas al sector turístico (transporte, alojamiento, restauración, intermediación, promoción turística, ocio, etc.) tienen a su disposición diferentes servicios *cloud* para gestionar de manera automática múltiples tareas relacionadas con su operativa empresarial. Los pequeños empresarios turísticos suelen contratar aplicaciones *cloud* de correo electrónico, gestión de recursos empresariales (ERP), tratamiento de información de clientes (CRM), suites ofimáticas, almacenamiento remoto y bases de datos en la nube, entre otros.

Además de compartir la problemática común de la contratación de servicios *cloud*, (propiedad intelectual, limitaciones y exclusiones de responsabilidades, límites en el ejercicio de acciones, etc.), el pequeño empresario turístico se enfrenta a cuestiones especialmente relacionadas con particularidades de su actividad.

En primer lugar, tras el examen de diferentes contratos *cloud* hemos

CONCLUSIONES

constatado que puede resultar difícil efectuar una distinción entre contratos *cloud* y las licencias de uso de software. Tras determinarse en capítulos anteriores la naturaleza jurídica del contrato de servicios de nube pública y sus diferencias con las licencias de uso de software, se recuerdan en este apartado las diferencias existentes entre el servicio *cloud* y el tradicional software *offline*, y cómo la licencia software forma parte de muchos de servicios *cloud* que implican la instalación en los propios equipos de programas informáticos por el empresario turístico.

Por otra parte, el empresario turístico puede almacenar datos relacionados con su actividad empresarial en servicios *cloud*, y por ello debe adoptar ciertas precauciones, tales como mecanismos de control de acceso por categorías laborales, una eficaz política de copias de seguridad y de recuperación de datos, o mecanismos de cifrado de información cuando el proveedor *cloud* no los proporcione por defecto. Es recomendable asimismo que contrate con un proveedor que pueda ofrecerle soporte técnico y servicios de consultoría, y que se asegure de las distribuciones de riesgos existentes entre el proveedor *cloud*, eventuales intermediarios y subproveedores del servicio, y aquellos riesgos que asume como suscriptor.

Puesto que el empresario turístico puede manejar considerables cantidades de datos personales de sus clientes, algunos de ellos incluso de carácter sensible, se ve obligado a prestar una especial atención tanto a aspectos relacionados con la seguridad de la información y con el cumplimiento de la normativa en materia de protección de datos. Al no poder negociar el contrato, deberá extremar su diligencia en la elección del proveedor. Asimismo, está obligado a recabar el consentimiento de los titulares de datos personales, en su papel de responsable del tratamiento, debiendo cumplir con lo establecido en la LOPD, entre ellos el consentimiento respecto de cesiones de datos y accesos por terceros (turoperadores, agencias de viajes, otros establecimientos o prestadores de servicios turísticos, asesorías, mutuas de salud, etc.). Cuando sea de aplicación en nuevo Reglamento General de Protección de Datos Personales, deberá informar a los interesados cuyos datos se traten mediante sistemas de computación en la nube que impliquen transferencias internacionales de datos, junto con las garantías de tales transferencias (*Shield*, cláusulas tipo, etc.), y recabar su consentimiento al respecto. La AEPD también recomienda que recabe el consentimiento del titular cuando elabore perfiles basados en los gustos y preferencias de los clientes. Asimismo, el documento de seguridad debe recoger las medidas de seguridad que implemente en el tratamiento de datos personales, y las eventuales incidencias que puedan tener lugar en el uso de servicios

CONCLUSIONES

de computación en la nube. Una vez finalizadas las operaciones de tratamiento de datos personales, deben inhabilitarse o borrarse los datos no necesarios, lo cual incluye aquellos que puedan estar almacenados remotamente.

El sector turístico resulta especialmente sensible a los picos estacionales de demanda. Si bien la computación en la nube es una solución idónea, al proporcionar un servicio elástico y escalable de capacidades, la caída del servicio puede obstaculizar seriamente la operativa empresarial y provocar pérdidas de ingresos y efectos negativos en la reputación empresarial. Por ello resulta especialmente importante el objetivo de nivel de servicio consistente en el parámetro de disponibilidad, que permite determinar la continuidad del servicio y la entrada en juego de compensaciones cuando se incumplan los objetivos mínimos marcados por el proveedor al respecto.

Por su relevancia en el sector turístico, hemos considerado adecuado hacer algunas breves referencias sobre ciertas plataformas Web 2.0 relacionados con el mundo del turismo. Las condiciones de uso de estas plataformas pueden presentar características comunes a los contratos de computación en la nube (propiedad intelectual, cumplimiento de PUA), y suponer otros problemas al empresario turístico. Se ponen de manifiesto cuestiones como los efectos legales de opiniones vertidas por internautas y sus consecuencias en la reputación empresarial, y exclusiones de responsabilidad respecto de la información publicada en plataformas cuya actividad no resulte totalmente ajena a la contratación entre turista internauta y establecimiento turístico.

CONCLUSIÓN FINAL. Para acabar con este trabajo, queremos poner de relieve la necesidad de una toma de conciencia por parte del pequeño empresario, pertenezca o no al sector turístico, de los riesgos que se derivan de la contratación de servicios de computación en la nube. Riesgos que nacen, por una parte, de la imposibilidad de negociar el contrato y de la falta de información técnica y legal sobre el servicio que suele existir al suscribirlo; por otra parte, de la posición débil del pequeño empresario, quien a diferencia del consumidor carece de protección legal específica, y por último, de la existencia de eventuales prácticas abusivas en el sector de la contratación de servicios *cloud*. Por ello, abogamos por una aplicación extensiva de la abusividad de ciertas cláusulas en aquellos casos en los que la situación del empresario pueda equipararse a la del consumidor (falta de conocimiento técnico, imposibilidad de negociación, necesidad del servicio que

CONCLUSIONES

contrata, etc.), por una mayor transparencia contractual y, en última instancia, por una regulación del contrato de servicios de computación en la nube en futuras normas mercantiles.

BIBLIOGRAFÍA

Bibliografía española

Monografías

ALBIEZ DOHRMANN, Klaus Jochen; *La protección jurídica de los empresarios en la contratación de condiciones generales*, 1ª edición, Navarra, 2009, 333 págs.

ALFARO ÁGUILA-REAL, Jesús, *Las condiciones generales de la contratación. Estudio de las disposiciones generales*, 1ª edición, Madrid, 1991, 482 págs.

APARICIO VAQUERO, Juan Pablo, *Licencias de uso no personalizadas de programas de ordenador*, 1ª edición, Granada, 2004, 424 págs.

APARICIO VAQUERO, Juan Pablo, *La nueva contratación informática. Introducción al outsourcing de los sistemas de información*, 1ª edición, Granada, 2002, 216 págs.

BADOSA COLL, Ferrán, *Dret d'Obligacions*, 1ª edición, Barcelona, 1990, 392 págs.

BAINBRIDGE, David; *Software Copyright Law*, 3ª edición, Londres, 1997, 389 págs.

BARRIUSO RUIZ, Carlos; *La contratación electrónica*, 3ª edición, Madrid, 2006, 780 págs.

BELTRÁN PARDO, Marta; SEVILLANO JAEN, Fernando; *Cloud Computing. Tecnología y negocio*, 1ª edición, Madrid, 2013, 167 págs.

CARRASCOSA LÓPEZ, Valentín; POZO ARRANZ, M^a Asunción; RODRÍGUEZ DE CASTRO, Eduardo P.; *La contratación informática: El nuevo horizonte contractual (los contratos electrónicos e informáticos)*, 2ª edición, Granada, 1999.

CASTÁN TOBEÑAS, José; *Derecho Civil Español, común y foral*, 15ª edición, Madrid, 1993, 1090 págs.

CLAVERÍA GOSÁLBEZ, Luís Humberto; *Condiciones Generales y cláusulas contractuales impuestas*, 1ª edición, Barcelona, 2008, 79 págs.

BIBLIOGRAFÍA

DAVARA RODRÍGUEZ, Miguel A, *Manual de Derecho Informático*, 10ª edición edición, Pamplona, 2015, 528 págs.

DE MIGUEL ASENSIO, Pedro A., *Derecho Privado de Internet*, 4ª edición, Pamplona. 2011, 1058 págs.

DEL PESO NAVARRO, Emilio, *Manual de outsourcing informático*, 2ª edición, Madrid, 2003, 272 págs.

DIEZ-PICAZO, Luís. *Fundamentos de Derecho Civil Patrimonial, Tomo II: Las relaciones obligatorias*. 6ª edición, Navarra, 2013, 1104 págs.

DIEZ-PICAZO, Luís, *Fundamentos del Derecho Civil Patrimonial, Vol. I. Introducción. Teoría del contrato*, 6ª edición, Navarra, 2007, 658 págs.

DIEZ-PICAZO, Luís, *Derecho de daños*, Madrid, 1ª edición, 1999, 367 págs.

FERNÁNDEZ DEL MORAL RODRÍGUEZ, Lourdes, *El contrato de suministro. El incumplimiento*, Madrid, 1992, 480 págs.

FERNÁNDEZ RODRÍGUEZ, José Julio, *Secreto e intervención de las comunicaciones en Internet*, 1ª edición, Madrid, 2004, 199 págs.

FONS GÓMEZ, Fernando J, *Cloud Computing: caracterización de los impactos positivos obtenidos por la utilización del modelo Cloud Computing por las pymes, basado en la tipología de modelos de negocio de este tipo de empresas* (Tesis de Máster), Universidad Politécnica de Valencia, Valencia, 2014. Disponible en: <<http://hdl.handle.net/10251/38864>>. [Fecha de consulta: 24 de mayo de 2017].

GARCÍA AMIGO, Manuel, *Cláusulas limitativas de la responsabilidad contractual*, 1ª edición, Madrid, 1965, 274 págs.

GARCÍA MEIXIA, Pablo; *Derechos y libertades, Internet y TICs*, 1ª edición, Valencia, 2014, 93 págs.

GÓMEZ CALERO, Juan, *Contratos mercantiles con cláusula penal*, 1ª edición, Madrid, 1983, 224 págs.

GUASCH PORTAS, Vicente, *La transferencia internacional de datos en las normativas española y comunitaria*, 1ª edición, Madrid, 2014, 336 págs.

HERNANDO COLLAZOS, Isabel; *Contratos informáticos. Derecho informático, legislación y práctica*, 1ª edición, San Sebastián, 1995, 914 págs.

JOYANES AGUILAR, Luis; *Computación en la nube. Estrategias de Cloud*

BIBLIOGRAFÍA

Computing en las empresas, 1ª edición, Barcelona, 2013, 518 págs.

LLANEZA GONZÁLEZ, Paloma, *E-contratos*. 1ª edición, Barcelona, 2004, 397 págs.

LLANEZA GONZÁLEZ, Paloma, *Aplicación práctica de la LSSI-CE*, 1ª edición, Barcelona, 2003, 363 págs.

LLODRÁ GRIMALT; Francisca; *El contrato celebrado bajo condiciones generales*, Valencia, 1ª edición, 2002, 436 págs.

LÓPEZ CALVO, José, *Comentarios al Reglamento Europeo de Protección de Datos*, 1ª edición, Madrid, 2017, 329 págs.

MARTÍN SANTISTEBAN, Sonia; *El depósito y la responsabilidad del depositario*, 1ª edición, Navarra, 2002, 291 págs.

MARTINEZ MARTÍNEZ, Ricard [et. al.]; *Derecho y Cloud Computing* (Coord.: Ricard Martínez), 1ª edición, Navarra, 2012, 307 págs.

MENÉNDEZ MATO, Juan Carlos, *El contrato vía Internet*, 1ª edición, Barcelona, 2005, 446 págs.

MORALES QUINTANILLA, Carlos René, "Las condiciones generales de los contratos y el control del contenido frente a las cláusulas abusivas", tesis doctoral inédita, Universidad de Salamanca, Facultad de Derecho, Salamanca, 2014.

MORENO NAVARRETE, M. Ángel, *Derecho-e, Derecho del comercio electrónico*, 1ª edición, Barcelona, 2002, 201 págs.

NEBREDÁ PÉREZ, Joaquín, *Distribución eléctrica. Concurrencia de disciplinas jurídicas*, 2ª edición, Madrid, 2003, 1028 págs.

OZCÁRIZ MARCO, Florencio; *El contrato de depósito. Estudio de la obligación de guarda*, 1ª edición, Barcelona, 1996, 350 págs.

PAGADOR LÓPEZ, Javier; *Condiciones Generales y cláusulas contractuales predispuestas*, Madrid, 1ª edición, 1999, 786 págs.

PANIZA FULLANA, Antonia, *Contratación a distancia y defensa de los consumidores*, 1ª edición, Granada, 2003, 432 págs.

PARDO GATO, José Ricardo, *Las páginas web como soporte de condiciones generales contractuales*, 1ª edición, Navarra, 2003, 158 págs.

BIBLIOGRAFÍA

PARDO GATO, José Ricardo, *Las cláusulas abusivas en contratos de adhesión*, 1ª edición, Madrid, 2004, 745 págs.

PLAZA PENADÉS, Javier, *Propiedad Intelectual y Sociedad de la Información*, 1ª edición, Navarra, 2002, 343 págs.

POLO, Eduardo, *Protección del contratante débil y condiciones generales de los contratos*, 1ª edición, Madrid, 1990, 138 págs.

PUYOL MONTERO, Javier; *Aproximación jurídica y económica al Big Data*, 1ª edición, Valencia, 2015, 356 págs.

PUYOL MONTERO, Javier, *Algunas consideraciones sobre Cloud Computing*, 1ª edición, Madrid, 2013, 276 págs.

RIBAS ALEJANDRO, Javier, *Aspectos jurídicos del comercio electrónico en Internet*, 1ª edición, Pamplona, 1999, 294 págs.

SÁNCHEZ LERÍA, Reyes, *El contrato de hospedaje de página web*, 1ª edición, Valencia, 2011, 283 págs.

SÁNCHEZ ROMÁN, Felipe, *Estudios de Derecho Civil*, Vol. I, 2ª edición, Madrid, 1899, 622 págs.

SERRA RODRÍGUEZ, Adela, *Cláusulas abusivas en la contratación. En especial, las cláusulas limitativas de responsabilidad*, 2ª edición, Pamplona, 2002, 250 págs.

SOLER MATUTES, Pere; *El contrato para la elaboración de programas de ordenador. Contrato de desarrollo de software*, 1 edición, Navarra, 2004, 298 págs.

TORRE DE SILVA, Javier, *Internet, Propiedad Industrial y Competencia Desleal*, Madrid, 2002, 159 págs.

TORRES VINYALS, Jordi; *Empresas en la nube. Ventajas y retos del Cloud Computing*, 1ª edición, 2011, Barcelona, 163 págs.

TRONCOSO REIGADA, Antonio; *La protección de datos personales. En busca del equilibrio*, 1ª edición, Valencia, 2010, 190 págs.

VEGA VEGA, José Antonio, *Contratos electrónicos y protección de los consumidores*, 1ª edición, Madrid, 2005, 495 págs.

YANGUAS GÓMEZ, Roberto, *Contratos de conexión a Internet, Hosting y*

BIBLIOGRAFÍA

búsqueda, 1ª edición, Navarra, 2012, 576 págs.

Obras colectivas, artículos y capítulos de libro

AA.VV., *Comentarios a la Ley de Condiciones Generales de la Contratación* (Coord. Rodrigo Bercovitz), Navarra, 1ª edición, 2000, 1548 págs.

AA.VV., *La defensa de los consumidores y usuarios. Comentario sistemático del texto refundido aprobado por el Real Decreto Legislativo 1/2007* (Dir. Manuel Rebollo Puig, Manuel Izquierdo Carrasco), Madrid, 1ª edición, 2011, 2088 págs.

AA. VV., *Lecciones de Responsabilidad Civil* (Coord. Fernando Reglero, José Manuel Busto), Navarra, 2ª edición, 2002, 656 págs.

AA. VV., *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (Dir. José Luis Piñar Mañas), Madrid, 1ª edición, 2016, 856 págs.

AA. VV., *Tratado de responsabilidad civil, Tomo II* (Coord. Fernando Reglero, José Manuel Busto), Navarra, 5ª edición, 2014, 2148 págs.

AA.VV., *Turismo y Nuevas Tecnologías*, (Coord. Apol·lònia Martínez), Navarra, 1ª edición, 2016, 209 págs.

ACEBEDO REBHEIN, Alberto, "Los mejores esfuerzos (best efforts) en el Derecho contemporáneo de los contratos", *Revista Estudios Socio-jurídicos*, 2006, Vol. 8, núm. 2, págs. 102-117.

ADSUAR PRIETO, Yolanda, "Cloud Computing vs. Protección de datos de carácter personal", *Actualidad Jurídica Aranzadi*, núm. 846, 2012.

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, págs. 63 a 81.

ALAMILLO DOMINGO, Ignacio; URIOS APARICI, Xavier; *Aspectes jurídics de la prestació de serveis públics emprant computació al Cloud* [en línea], Generalitat de Catalunya, 2012. Disponible en: <http://eapc.gencat.cat/web/.content/home/recerca-antiga/treballs_de_recerca_subvencionats/treballs_de_recerca_realitzats/2011/mixtos/m01_urios_sintesi.pdf>. [Fecha de consulta: 2 de agosto de 2016]

ALARCÓN FIDALGO, Joaquín; "Cloud Computing, responsabilidad y

BIBLIOGRAFÍA

seguro", *Revista Española de Seguros: Publicación Doctrinal de Derecho y Economía de los Seguros Privados*, núm. 153-154, 2013, págs 29 a 42.

ALFARO AGUILA-REAL, Jesús, "Cláusulas abusivas, cláusulas predisuestas y condiciones generales", *Anuario Jurídico de La Rioja*, núm. 4, 1998, págs. 53 a 70.

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, págs. 103 a 140.

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, 1000 págs.

ÁLVAREZ LATA, Natalia [et al.]; "Contratos de prestación de servicios y realización de obras. 2.- Servicios de guarda y custodia" (Dir. Rodrigo Bercovitz), *Tratado de contratos*, Vol. III 1ª edición, Valencia, 2009, págs. 2913 a 3008.

ÁLVAREZ RIGAUDIAS, Cecilia, "Condiciones para las transferencias internacionales de datos personales en servicios Cloud", *Derecho y Cloud Computing* (Coord. Ricard Martínez Martínez), 1ª edición, Navarra, 2012, págs. 109 a 148.

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].

APARICIO VAQUERO, Juan Pablo, "Cuestiones de Derecho aplicable y responsabilidad de los prestadores de servicios de red social y sus usuarios", *En torno a la privacidad y la protección de datos de la sociedad de la información* (Coord. Alfredo Batuecas, Juan Pablo Aparicio), Granada, 2015, págs. 187 a 231.

APARICIO VAQUERO, Juan Pablo, "El cese en la prestación de servicios de acceso a Internet", *Actas de Derecho Industrial y Derecho de Autor*, núm. 34, 2013-2014, págs. 619 a 623.

APARICIO VAQUERO, Juan Pablo, "Negocios y contratación en Internet. El ejemplo de los portales de ocio y viajes", en *FODERTICS, estudios sobre Derecho y Nuevas Tecnologías* (Coord. Federico Bueno de Mata), La Coruña, 2012, págs. 53 a

BIBLIOGRAFÍA

78.

APARICIO VAQUERO, Juan Pablo, "Autorregulación de Internet y resolución extrajudicial de conflictos", *Autores, consumidores y comercio electrónico*, (Coord. Juan Pablo Aparicio, Alfredo Batuecas), Madrid, 2004, págs. 471 a 510.

AREITIO BERTOLÍN, Javier, *Protección del Cloud Computing en Seguridad y privacidad*, Revista Española de Electrónica, núm. 666, 2010, págs 42 a 48.

ARIAS DE RINCÓN, María Inés; "La calificación jurídica de las transmisiones de software en Internet", *Revista de filosofía jurídica, social y política*, Vol. 14, núm. 1, 2007, págs 9-31.

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. 1194 a 1210.

BADENAS CARPIO, Juan, "Ámbito Subjetivo de la Ley de Condiciones Generales de la Contratación", *Comentarios a la Ley de Condiciones Generales de la Contratación* (Coord. Rodrigo Bercovitz Rodríguez-Cano), 1ª edición, Navarra, 2000, 1548 págs.

BATUECAS, Alfredo; APARICIO, Juan P., "La contratación *on line* de servicios turísticos", *Nuevas fórmulas de comercialización "on line" de servicios turísticos, subsunción en los tipos legales y distribución de responsabilidad* (Coord. Antonia Paniza), Granada, 2013, págs. 49 a 78.

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, págs 13-60.

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 a 20.

BESTUE SALINAS, Carmen, "Traducir los daños sin efectos colaterales: análisis comparado del Derecho de Daños", *Hermeneus Revista de Traducción e Interpretación*, núm. 11, 2009, págs 81 a 107.

BORETTO, Mónica M.; *Aspectos de la propiedad intelectual derivados del entorno digital* [en línea]. Disponible en: <www.eumed.net/libros/2005/mmb/>.

BIBLIOGRAFÍA

[Fecha de consulta: 15 de agosto de 2016].

CÁMARA 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].

CAMPANILLAS CIAURRIZ, Jorge, *El big data y la impugnación de valoraciones de la LOPD, una aproximación* [en línea]. Disponible en: <<http://www.iurismatica.com/el-big-data-y-la-impugnacion-de-valoraciones-de-la-lopd-una-aproximacion/>>. [Fecha de consulta: 14 de septiembre de 2016].

CAÑIZARES LASO, Ana; DE PABLO CONTRERAS, Pedro; ORDUÑA MORENO, Javier; VALPUESTA FERNÁNDEZ, Rosario (Dir. Rosario Valpuesta Fernández), *Código Civil Comentado, Volumen III. Libro IV-Obligaciones y contratos*, 2ª edición, Navarra, 2016, 1272 págs.

CARBAJO CASCÓN, Fernando, "La propiedad intelectual como objeto del comercio electrónico", *Autores, consumidores y comercio electrónico* (Dir. María Jesús Moro Almaraz), Madrid, 2004, págs. 51 a 105.

CASTILLO JIMENEZ, Cinta, "Protección del derecho a la intimidad y uso de las nuevas tecnologías de la información", *Revista Derecho y conocimiento de la Facultad de Derecho de la Universidad de Huelva*, Vol. 1, 2001, págs. 35 a 48.

CASTILLO PARRILLA, José Antonio, "El contrato de suministro de contenidos digitales y los contratos de desarrollo de software y creación web en el Derecho de consumidores. De la Propuesta CESL y la Directiva 2011/83/UE a la Propuesta de Directiva 634/2015, de 9 de diciembre", *Revista CESCO de Derecho de Consumo*, núm. 17, 2016, págs. 45 a 61.

CASTILLO PARRILLA, José Antonio, "La previsible evolución de la regulación de los contenidos digitales en el Derecho de la Unión Europea (Propuesta Directiva 634/2015, de 9 de diciembre, sobre ciertos aspectos relativos al suministro de contenidos digitales)", *Revista Lex Mercatoria*, núm. 1, 2016, págs 12-16.

CAZURRO BARAHONA, Víctor, "Transferencias Internacionales de datos", *Grandes Tratados. Prácticum Protección de datos*, Navarra, 2015, págs. 390 a 441.

COBAS COBIELLA, Maria Elena, "Derecho al olvido: de la STJUE de 2014 al

BIBLIOGRAFÍA

Reglamento Europeo de Protección de Datos", *Actualidad Civil*, núm. 1, 2017, págs 98 a 116.

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].

CORONA HERRERO, Ulises J., "Los datos en la nube: retos actuales en la protección del Derecho de Propiedad", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 32, mayo-agosto 2013, págs. 69 a 82.

CORRIPIO GIL-DELGADO, Reyes; "Consideraciones jurídicas del contrato de Outsourcing", *Encuentros sobre Informática y Derecho de la Universidad Pontificia de Comillas 1997-1998*, Pamplona, 1998, págs 111 a 131.

CORTÉS, JAVIER, "Los contratos bancarios (II). Servicio de cajas de seguridad", *Lecciones de Derecho Mercantil* (Dir. Aurelio Menéndez), 13ª edición, Navarra, 2015, págs 719 a 738.

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, págs. 86 a 103.

DE CARLOS BERTRÁN, José Manuel; "El Outsourcing como técnica de gestión alternativa y su regulación contractual", *Derecho de los negocios*, núm. 91, Madrid, 1999, págs 9 a 32.

DE CASTRO, Federico, "Notas sobre las limitaciones intrínsecas a la autonomía de la voluntad. La defensa de la competencia. El orden público. La protección del consumidor", *Anuario de Derecho Civil*, 1982, págs. 987-1086.

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, págs 111 a 131.

DE MIGUEL ASENSIO, Pedro A., *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].

BIBLIOGRAFÍA

DÍEZ-PICAZO, Luis, "Cláusula penal y resolución del contrato", *Libro-Homenaje al profesor Amorós Guardiola*, Madrid, 2006, págs. 385 a 408.

DÍAZ DÍAZ, Efrén, "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones", *Revista Aranzadi Doctrinal*, núm. 6, 2016, págs 155 a 190.

DOMINGO, Miguel Á., CHÁVEZ, Esther; ESCOBAR, Bernabé, "Evolución del Software y herramientas de Revenue Management utilizados por hoteles", *Actas del XI Congreso Internacional de Turismo y Tecnologías de la Información y la Comunicación TuriTec*, 2016, Universidad de Málaga, págs. 484 a 503.

DOMÍNGUEZ LUELMO, Andrés; GUILARTE MARTÍN-CALERO, Cristina; IGLESIAS REBOLLO, César, *Nuevas Tecnologías y Propiedad Intelectual* (Coord. Carlos Rogel), 1ª edición, Madrid, 1999, 252 págs.

EBERS, Martin, "El control de las cláusulas abusivas en un futuro instrumento opcional", *InDret Revista para el análisis del Derecho* [en línea], núm. 1, 2012, 46 págs. Disponible en: <http://www.indret.com/pdf/881_es.pdf>. [Fecha de consulta: 4 de julio de 2016].

ECHAIDE IZQUIERDO, Juan Miguel; LARA GONZÁLEZ, Rafael, *Consumo y Derecho. Elementos jurídico-privados de Derecho de Consumo*, 1ª edición, Madrid, 2006, 394 págs.

ÉCIJA BERNAL, Álvaro; SÁIZ PEÑA, Carlos, *Contratos de Internet. Modelos y comentarios*, 1ª edición, Navarra, 2002, 429 págs.

ESCANDELL, Daniel. *Concepto "granja de servidores"* [en línea], 2012. Disponible en: <<http://revistacaracteres.net/campoconceptual/granja-de-servidores>>. [Fecha de consulta: 27 de junio de 2016].

ESTEBAN DE LA ROSA, Fernando; OLARIU, Ozana, "La propuesta de normativa común de compraventa europea y su aplicabilidad a los contratos de consumo", *La protección del consumidor en dos espacios de integración: Europa y América: Una perspectiva de Derecho internacional, europeo y comparado*, 1ª edición, Valencia, 2015, págs. 111 a 145.

FARRÉ TOUS Santiago, "Data breach notification, procedimiento sancionador y derecho a no confesarse culpable", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 26/2011, Pamplona, 2011, págs. 69 a 85.

BIBLIOGRAFÍA

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.

FERNÁNDEZ MASÍA, Enrique; "Optando por la normativa común de compraventa europea", *Revista Electrónica de Estudios Internacionales*, núm. 23, 2012. Disponible en: <<http://www.reei.org/index.php/revista/num23/notas/optando-normativa-comun-compraventa-europea>>. [Fecha de consulta: 24 de mayo de 2017].

FONTANELLAS MORELL, Josep; "La normativa común de compraventa Europea: ¿punto y final o punto y seguido?", *Anuario Español de Derecho Internacional Privado*, vol. XIV-XV, 2014-2015, págs. 447 a 489.

GARCÍA DEL POYO VIZCAYA, Rafael, "La contratación empresarial de servicios de *Cloud Computing*", *Derecho y Cloud Computing* (Coord. Ricard Martínez Martínez), 2012, Navarra, págs. 179 a 200.

GARCÍA DÍAZ, Margarita; HIDALGO RÚA, Gloria María, "Invenciones y creaciones intelectuales laborales: especial referencia al software", *Acciones e investigaciones sociales*, núm. 4, 1996, págs. 79 a 92.

GARCÍA MEIXIA, Pablo, "Cloud Computing: sus implicaciones legales", *Revista Aranzadi Derecho y Nuevas Tecnologías*, núm 23, 2010, págs. 79 a 91.

GARCÍA SÁNCHEZ, Manuel, "Retos de la computación en la nube", *Derecho y Cloud Computing* (Coord. Ricard Martínez Martínez), 1ª edición, Navarra, 2012, págs 37 a 60.

GÓMEZ PERALS, Miguel; "Algunos aspectos civiles de la contratación electrónica en materia de licencia de software", *Informática y Derecho: Revista Iberoamericana de Derecho Informático*, núm. 30-31-32, 1999, págs. 349 a 364.

GRIMALT SERVERA, Pedro, "La contratación en masa en Internet: el consentimiento de los consumidores para el tratamiento de sus datos en una condición general", *Autores, consumidores y comercio electrónico* (Dir. María Jesús Moro Almaraz), Madrid, 2004, págs. 235 a 249.

GONZÁLEZ, Javier, "¿Qué significa realmente el porcentaje de *Uptime*?" [en línea], *Blogs Teoriza de Tecnología e informática*, 2011. Disponible en: <<http://gonzo.teoriza.com/significa-realmente-porcentaje-uptime-burbuja-disponibilidad>>. [Fecha de consulta: 21 de marzo de 2017].

BIBLIOGRAFÍA

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.

GUASCH PORTAS, Vicent; SOLER FUENSANTA, José; "Cloud Computing, turismo y protección de datos", *Revista de Análisis Turístico*, núm. 17, 2014, págs. 61-68.

GUASCH PORTAS, Vicente, "La transferencia internacional de datos de carácter personal", *Revista de Derecho, UNED*, núm. 11, 2012, págs. 413 a 453.

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 a 332.

GUILLÉN CATALÁN, Raquel, "El valor de los votos particulares en la extensión del control de transparencia de la contratación entre empresarios", *Diario La Ley*, núm. 8841, 11 de octubre de 2016.

GUIX TORNOS, Anna; "Redes sociales y derechos de autor: ¿de quién son los contenidos?", *Actualidad jurídica Aranzadi*, núm. 879, Navarra, 2014, pág. 8.

JUNTA DE ANDALUCÍA; SOCIEDAD ANDALUZA PARA EL DESARROLLO DE LAS TELECOMUNICACIONES SANDETEL, *Cloud Computing aplicado a los sectores de la agroindustria, eficiencia energética, industrias culturales y turismo* [en línea], 2012. Disponible en: <http://www.juntadeandalucia.es/export/drupaljda/analisis_cloud_computing.pdf>. [Fecha de consulta: 21 de marzo de 2017].

LACITY, Mary C.; HIRSCHHEIM, Rudy, "Subcontratación de los sistemas de información: mitos y realidades", *Harvard-Deusto Business Review*, 1994, núm. 59, págs. 86 a 99.

LECUYER, Hervé, "Modificaciones unilaterales del contrato", *Revista de Derecho Privado*, núm. 21, 2011, págs. 257 a 272.

LEENES, Ronald, "¿Quién controla la nube?", *Revista de Internet Derecho y Política de la Universitat Oberta de Catalunya* [en línea], núm. 11, 2010. Disponible en: <<http://idp.uoc.edu/articles/abstract/10.7238/idp.v0i11.1081/>>. [Fecha de consulta: 24 de mayo de 2017].

LÓPEZ JIMENEZ, David; "La computación en la nube o cloud computing

BIBLIOGRAFÍA

examinada desde el ordenamiento jurídico español", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso XL*, Chile, 1er Semestre, págs. 689 a 709.

LÓPEZ JIMÉNEZ, David, "Los códigos de conducta como paradigma de buenas prácticas: el caso del comercio electrónico", *Encuentros multidisciplinares*, Vol. 11, núm. 32, 2009, págs. 49 a 55.

LÓPEZ JIMÉNEZ, David; MARTÍNEZ LÓPEZ, Fco. José, "Los códigos de conducta como solución frente a la falta de seguridad en materia de comercio electrónico", *Ciencias Económicas*, Vol. 28, núm. 1, 2010, págs.117 a 139.

LÓPEZ Y LÓPEZ, Ángel M, "Propiedad intelectual y perplejidades del derecho civil", *Cuestiones de actualidad en el ámbito de la propiedad intelectual* (Coord. Inmaculada Vivas), 1ª edición, Madrid, 2015, págs. 17 a 25.

MARCO ALCALÁ, Luis Alberto; "Contratos de Depósito y Contratos Análogos", *Contratos Mercantiles Vol. I*. (Coord. M^a Ángeles Calzada; Dir. Alberto Bercovitz), 5ª edición, Navarra, 2013, 1292 págs.

MARCO ALCALÁ, Luis Alberto; "Contratos de Depósito. Depósito en almacenes generales", *Contratos Mercantiles Vol. I*. (Coord. M^a Ángeles Calzada; Dir. Alberto Bercovitz), 6ª edición, Navarra, 2017, págs. 1005 a 1045.

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* [en línea]. Getafe, Universidad Carlos III de Madrid, 2015, págs. 1373 a 1387. Disponible en: <<http://hdl.handle.net/10016/21016>>. [Fecha de consulta: 1 de marzo de 2016].

MARTINEZ NADAL, Apol·lònia, "Publicación en páginas web de valoraciones falsas con incidencia en la reputación digital de los empresarios de alojamiento ¿una práctica desleal?", *Revista de Derecho Mercantil*, 2015, núm. 297, págs.139-169.

MARTÍNEZ NADAL, Apol·lònia, "Las cláusulas de paridad en las relaciones entre OTA (*Online Travel Agencies*) y empresarios de alojamiento turístico: presente y futuro", *Diario La Ley*, núm. 8574, 2015, págs. 1 y ss.

MARTÍNEZ NADAL, Apol·lònia, "Las centrales electrónicas de reservas turísticas: breves consideraciones acerca de su naturaleza y régimen jurídico", *Libro*

BIBLIOGRAFÍA

homenaje al Prof. Dr. José Antonio Gómez Segade (Coord. Ana María Tobío Rivas; Ángel Fernández-Albor Baltar, Anxo Tato Plaza), 2013, págs. 967 a 984.

MARTINEZ NADAL, Apol·lònia, "Reputación online de las empresas de alojamiento turístico y publicación por terceros de informaciones negativas (reviews)" [en línea], *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*, Universidad Carlos III de Madrid. Disponible en: <<http://hdl.handle.net/10016/21115>>. [Fecha de consulta: 23 de marzo de 2017].

MARTÍNEZ NADAL, Apol·lònia, "Las centrales electrónicas de reservas turísticas", *Estudios de Derecho Mercantil. Libro homenaje al Prof. J.A. Gómez Segade*, Madrid, 2013, págs. 967-984.

MARTÍNEZ NADAL, Apol·lònia, "Derecho de la competencia y cláusulas de paridad en la comercialización turística electrónica", *Turismo y Nuevas Tecnologías* (obra colectiva), Editorial Thomson Civitas, 2016, págs. 10 y ss.

MARTÍNEZ NADAL, Apol·lònia, ROSSELLÓ RUBERT, Francisca María, "La experiencia del cliente: análisis jurídico de la publicación online de comentarios de clientes. En particular, el caso de TripAdvisor", *Actas de las IX Jornadas de Investigación en Turismo*, Sevilla, 2016, págs. 99 a 128.

MARTÍNEZ NADAL, Apol·lònia, ROSSELLÓ RUBERT, Francisca María, "Comercio electrónico y Derecho de la Competencia: las cláusulas de paridad en el sector turístico", *Hacia una justicia 2.0. Actas del XX Congreso Iberoamericano de Derecho e Informática*, (Dir. Federico Bueno de Mata), Salamanca, 2016, págs. 387 a 402.

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*, Editorial Aranzadi, nº 26, 2011, págs 87 a 100.

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 a 229.

MASIDE MIRANDA, José Enrique, "La cláusula penal", *Libro-Homenaje al profesor Amorós Guardiola*, Madrid, 2006, págs. 497 a 524.

MATA GONZÁLEZ, Miguel Ángel, "¿En qué consiste el debate abierto sobre

BIBLIOGRAFÍA

la patentabilidad del software?" [en línea], *Revista Iuris*, núm. 78, Diciembre 2003. Disponible en: <<http://www.miguelangelmata.com/wp-content/uploads/2007/03/en-que-consiste-el-debate-abierto-sobre-la-patentabilidad-del-software-mm-g.pdf>>. [Fecha de consulta: 15 de agosto de 2016].

MATO PACÍN, Natalia, "El control de contenido en la contratación mediante condiciones generales entre empresarios en el Derecho comparado y europeo", *Cuadernos de Derecho Transnacional*, Octubre 2015, Vol. 7, núm. 2, págs. 216 a 282.

MEGÍAS QUEIRÓS, José Justo, "Vida privada y nuevas tecnologías", *Revista de la contratación electrónica*, núm. 17, 2007, págs. 3 a 28.

MENDOZA LOSANA, Ana I, "Ofertas "para toda la vida" y modificación de condiciones de los contratos de servicios de telecomunicaciones", *Centro de estudios de consumo de la Universidad de Castilla la Mancha* [en línea]. Disponible en: <<https://www.uclm.es/centro/cesco/pdf/trabajos/29/OfertasTodavida.pdf>>. [Fecha de consulta: 20 de febrero de 2017].

MENDOZA LOSANA, Ana I, "Modificación unilateral de precios en contratos de duración indeterminada", *Análisis Gómez-Acebo y Pombo* [en línea], 2013. Disponible en: <<http://www.gomezacebo-pombo.com/media/k2/attachments/modificacion-unilateral-de-precios-en-contratos-de-duracion-indeterminada.pdf>>. [Fecha de consulta: 20 de febrero de 2017].

MENDOZA LOSANA, Ana I, "Control de condiciones generales de la contratación en sectores regulados. en particular, la cláusula que permite la modificación unilateral de los precios", *Centro de Estudios de Consumo de la Universidad de Castilla la Mancha*, [en línea]. Disponible en: <<https://www.uclm.es/centro/cesco/pdf/trabajos/30/22.pdf>>. [Fecha de consulta: 20 de febrero de 2017].

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 a 44.

MIQUEL GONZALEZ, José María, "La nulidad de las condiciones generales", *Las nulidades de los contratos: un sistema en evolución* (Coord. J. Delgado Echeverría), Navarra, 2007, págs. 193 a 233.

MINERO ALEJANDRE, Gemma, "A vueltas con el Derecho al Olvido. Construcción normativa y jurisprudencial del derecho de protección de datos de

BIBLIOGRAFÍA

carácter personal en el entorno digital", *Revista Jurídica de la Universidad Autónoma de Madrid*, núm. 20, 2014, págs. 129 a 155.

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].

MIRALLES, Ramón; *El derecho de la portabilidad de datos personales* [en línea]. Disponible en: <<http://www.abogacia.es/2012/11/15/el-derecho-de-la-portabilidad-de-los-datos-personales/>>. [Fecha de consulta: 20 de febrero de 2017].

MIRALLES; Ramón, *Big Data vs Small Law* [en línea]. Disponible en: <<http://www.abogacia.es/2013/07/10/big-data-vs-small-law/>>. [Fecha de consulta: 14 de septiembre de 2016].

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].

MORALES, Juan Ramón, "Cloud computing: riesgos corporativos e implicaciones jurídicas" [en línea]. *Actualidad Jurídica Aranzadi*, núm. 863. Disponible en: <<http://www.garrigues.com/es/publicaciones/articulos/Paginas/Cloud-computing-riesgos-corporativos-e-implicaciones-juridicas.aspx>>. [Fecha de consulta: 17 de enero de 2017].

MORO ALMARAZ, M^a Jesús, "Servicios de la Sociedad de la Información y sujetos intervinientes", *Autores, consumidores y comercio electrónico* (Dir. María Jesús Moro Almaraz), Madrid, 2004, págs. 107 a 140.

NAVAS NAVARRO, Susana, "Computación en la nube: Big Data y Protección de Datos Personales" [en línea], *InDret Revista para el análisis del Derecho*, núm. 4/2015, 2015. Disponible en: <http://www.indret.com/pdf/1193_es.pdf>. [Fecha de consulta: 12 de septiembre de 2016].

NEGRÍN RUIZ, Anisley; PÉREZ PEÑA, Óscar Alberto; "¿Corolario de los derechos de autor del software?", *Autor y derecho. Ciberrevista sobre propiedad*

BIBLIOGRAFÍA

intelectual, Universidad de La Rioja, núm. 3, 2004, págs. 1 a 16. Disponible en: <http://www.unirioja.es/dptos/dd/civil/autor_anisley.pdf>. [Fecha de consulta: 9 de agosto de 2016].

OTTO, Carlos; *Las startups 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: 28 de julio de 2016].

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.

PAGADOR LÓPEZ, Javier, "Condiciones generales y cláusulas abusivas", *Defensa de los Consumidores y Usuarios. Comentario sistemático del texto Refundido aprobado por Real Decreto 1/2007* (Dir. Rebollo Puig, Izquierdo Carrasco), Madrid, 2011, 2088 págs.

PALOMAR OLMEDA, Alberto; "Incidencia del *Cloud Computing* en el ámbito de la contratación pública", *Derecho y Cloud Computing* (Coord. Ricard Martínez), 1ª edición, Navarra, 2012, págs 201 a 230.

PALOS SÁNCHEZ, Pedro R.; AGUAYO CAMACHO, Mariano, *Los ecosistemas de Turismo Inteligente basados en Cloud Computing*, *El Turismo y la experiencia del cliente, Actas de las IX Jornadas de Investigación en Turismo*, Tomo II, Universidad de Sevilla, 2016, págs. 125-146.

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.

PAYERAS, Magdalena; CAVANILLAS, Santiago, "Los servidores de acceso y alojamiento: descripción técnica y legal", *Deberes y responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar* (Coord. Santiago Cavanillas), Granada, 2005, págs 1 a 28.

PEGUERA POCH, Miguel, "La exención de responsabilidad civil por contenidos ajenos en Internet", *Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet*, (Coord. Fermín Morales, Óscar Morales), 1ª edición, Navarra, 2002, págs. 25 a 64.

BIBLIOGRAFÍA

PEREDA, Cristina F; *Las claves de las leyes SOPA y PIPA* [en línea], 2012. Disponible en: <http://tecnologia.elpais.com/tecnologia/2012/01/19/actualidad/1326967261_850215.html>. [Fecha de consulta: 15 de agosto de 2016].

PLA OCÁÑEZ, Guillermo; LÓPEZ-BAILLO, Berta; *Data mining: protección de datos y comercio electrónico* [en línea]. Disponible en: <<http://www.togas.biz/articulos/TIC/Proteccion-de-Datos/Data-Mining--Proteccion-de-datos-y-comercio-electronico.html>>. [Fecha de consulta: 15 de agosto de 2016].

PLAZA PENADÉS, Javier, "Doctrina del Tribunal Supremo sobre el "conocimiento efectivo" en la responsabilidad de los prestadores intermediarios y en el derecho al olvido", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 34, 2014, págs. 15 a 19.

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.

RAMÍREZ, Pablo; "Oracle vs Google: las APIs son (definitivamente) protegibles por copyright" [en línea], *Blog Cuatrecasas Gonçalves Pereira Propiedad Intelectual*. Disponible en: <<http://cuatrecasasblog.com/propiedad-intelectual/oracle-vs-google-las-apis-son-definitivamente-protegibles-por-copyright/>>. [Fecha de consulta: 15 de agosto de 2016].

REBOLLO PUIG, Manuel, IZQUIERDO CARRASCO, Manuel, *La defensa de los consumidores y usuarios. Comentario sistemático del texto refundido aprobado por Real Decreto Legislativo 1/2007, 1ª edición*, Madrid, 2011, 2088 págs.

ROSSELLÓ RUBERT, Francisca M^a, "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.

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.

ROSSELLÓ RUBERT, Francisca M^a; "La transferencia de datos personales entre PYMEs españolas y proveedores norteamericanos de *Cloud Computing* tras la

BIBLIOGRAFÍA

reciente anulación del Acuerdo Safe Harbor por el Tribunal de Justicia de la Unión Europea", *Diario La Ley*, núm. 8725, 2016.

RUBÍ NAVARRETE, Jesús, "El proveedor de *cloud* como encargado del tratamiento", *Derecho y Cloud Computing*, (coord. Ricard Martínez), Navarra, 2012, págs. 87 a 108.

SAIZ PEÑA, Carlos Alberto, "La notificación de brechas de seguridad", *Hacia un nuevo Derecho europeo de Protección de Datos*, Valencia, 2015, págs. 771 a 817.

SAIZ PEÑA, Carlos A, "Medidas de seguridad en el Cloud Computing", *Derecho y Cloud Computing* (coord. Ricard Martínez), 1ª edición, Navarra, 2012, págs. 149 a 178.

SÁNCHEZ CALERO, Fernando; SÁNCHEZ-CALERO ULLARTE, Juan; *Instituciones de Derecho Mercantil*, Vol. II, 37ª edición, Navarra, 2015, 758 págs.

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 3 a 30.

SÁNCHEZ MARTÍN, Carlos, "El verdadero control de transparencia de las cláusulas predispuestas. Su definitiva plasmación y fundamentación técnica", *Diario La Ley*, núm. 8491, Sección Tribuna, 2 de marzo de 2015.

SÁNCHEZ MARTÍN, Carlos, "La contratación bajo condiciones generales de la contratación frente a la contratación por negociación. Sus mecanismos específicos de control: abusividad y transparencia. La eficacia contractual resultante tras la declaración de abusividad", *Diario La Ley*, núm. 8333, Sección Tribuna, 16 de junio de 2014.

SPINDLER, Gerald, "Contratos de suministro de contenidos digitales: ámbito de aplicación y visión general de la Propuesta de Directiva de 9.12.2015", *Indret Revista para el análisis del Derecho*, núm. 3, 2016, [en línea]. Disponible en: <<http://www.indret.com/pdf/1243.pdf>>. [Fecha de consulta: 26 de enero de 2017].

TIMPANARO RONCERO, Salvador, "Las condiciones generales de la contratación y cláusulas abusivas", *Las condiciones generales de la contratación y cláusulas abusivas* (Coord. Luís Díez-Picazo, Fernando Sánchez Calero, *et.al.*), Madrid, 1996, págs. 289 a 328.

TRONCOSO REIGADA, Antonio, "Las redes sociales a la luz de la propuesta

BIBLIOGRAFÍA

de Reglamento General de Protección de Datos Personales. Parte dos", *Revista d'Internet, Dret i Política*, núm. 16. 2013, págs. 27 a 39.

TUR FÁUNDEZ, M^a Nélica, "La responsabilidad contractual de los intermediarios electrónicos", *Deberes y Responsabilidades de los servidores de acceso y alojamiento. Un análisis multidisciplinar* (Coord. Santiago Cavanillas), Granada, 2005, págs. 145 a 164.

VALDECANTOS FLORES, Maitane; *Talento TIC: la protección del programa de ordenador* [en línea]. [Fecha de consulta: 15 de agosto de 2016]. Disponible en: <http://tecnologia.elderecho.com/tecnologia/propiedad_intelectual_e_industrial/Talento-TIC-proteccion-Programa-Ordenador_11_620305002.html>.

VALERO TORRIJOS, Julián; "La Administración Pública en la nube. Análisis de las implicaciones jurídicas desde la normativa sobre Administración electrónica", *Derecho y Cloud Computing* (Coord. Ricard Martínez), 1^a edición, Navarra, 2012, págs. 231 a 255.

VALPUESTA GASTAMINZA, Eduardo, "La Propuesta de Normativa Común de Compraventa Europea (CESL), un paso más hacia la unificación del derecho de contratos en la unión europea, lastrado por la protección al consumidor", *Cuadernos de Derecho Transnacional*, Vol. 5, 2013, págs. 199 a 216.

VAQUERO PINTO, M^a José, "Contrato de servicios", *Contratos Mercantiles, Vol. I.* (Coord. M^a Ángeles Calzada; Dir. Alberto Bercovitz), 6^a edición, Navarra, 2017, págs. 931 a 965.

VAQUERO PINTO, María José; "Contratos de prestación de servicios y realización de obras", *Tratado de contratos*, Vol. III (Dir. Rodrigo Bercovitz), 2^a edición, Valencia, 2013, 6892 págs.

VÁZQUEZ RUANO, Trinidad, "La autorregulación en la propuesta de Código Mercantil", *Estudios sobre el futuro Código Mercantil: libro homenaje al profesor Rafael Illescas Ortiz*. Getafe [en línea], 2015, págs. 327 a 346. Disponible en: <<http://hdl.handle.net/10016/20763>>. [Fecha de consulta: 17 de enero de 2017].

VIGUIRI CORDERO, Jorge; "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", *Hacia un nuevo Derecho europeo en protección de datos*, 1^a edición, Valencia, 2015, págs. 901 a 957.

VICENT CHULIÀ, Eduardo; BELTRÁN ALANDETE, Teresa; *Aspectos*

BIBLIOGRAFÍA

jurídicos de los contratos atípicos; 4ª edición, Barcelona, 1999, 448 págs.

VIVAS TESÓN, Inmaculada, "La doble protección jurídica de las bases de datos: derecho de autor y derecho sui generis del fabricante", *Cuestiones de actualidad en el ámbito de la propiedad intelectual* (Coord. Inmaculada Vivas), 1ª edición, Madrid, 2015, págs. 145 a 173.

XALABARDER PLANTADA, Raquel; *Derechos de autor: ley aplicable y jurisdicción competente en la era digital* [en línea]. Disponible en: <<http://www.uoc.edu/web/esp/art/uoc/0105020/xalabarder.html>>. [Fecha de consulta: 25 de junio de 2015].

XALABARDER PLANTADA, Raquel; "Redes sociales y Propiedad Intelectual", *Derecho y redes sociales*, (Coord. Artemi Rallo, Ricard Martínez), 1ª edición, Navarra, 2010, pág. 335 a 354.

XALABARDER PLANTADA, Raquel; "Las licencias Creative Commons: ¿una alternativa al *copyright*?" [en línea], 2006. Disponible en: <<http://www.uoc.edu/uocpapers/2/dt/esp/xalabarder.pdf>>. [Fecha de consulta: 9 de agosto de 2016].

YÁÑEZ DE ANDRÉS, Aquilino; "Autónomos y pequeños empresarios en la contratación seriada", *Diario La Ley*, núm. 8419, 12 de noviembre de 2014.

ZALAZAR, Ana S; GONNET, Silvio; LEONE, Horacio; "Aspectos contractuales del *Cloud Computing*", *Tercer Congreso Iberoamericano de investigadores y Docentes de Derecho e Informática*, [en línea]. Disponible en: <<http://www.ciiddi.org/congreso2014/images/documentos/aspectos%20contractuales%20de%20cloud%20computing%20zalazar.pdf>>. [Fecha de consulta: 2 de mayo 2016].

ZOCO ZABALA, Cristina, "Acceso a los datos ajenos “en la nube” e interceptación de las comunicaciones virtuales ajenas: diferente protección iusfundamental", *Actas VI Congreso Internacional Latina de Comunicación Social*, Universidad de La Laguna, diciembre 2014.

Bibliografía extranjera

Monografías

MARCHINI, Renzo; *Cloud Computing: a practical introduction to the legal*

BIBLIOGRAFÍA

issues, 1ª edición, Londres, 2010, 180 págs.

OPPENHEIM, Charles, *The non-sense guide to legal issues in web 2.0 and Cloud Computing*, 1ª edición, Londres, 2012, 125 págs.

SENFLEBEN, Martin, *Copyright, Limitations and the Three-Steps Test*, Kluwer Law International, La Haya, 2004, 340 págs.

STONE, Peter; *Copyright Law in the UK and European Community*, 1ª edición, Londres, 1990, 293 págs.

TOLLEN, David W., *The Tech Contracts Handbook*, Illinois, 2015, 281 págs.

Obras colectivas, artículos y capítulos de libro

ADAMS, Kenneth A., *Understanding "Best Efforts" and Its Variants, (Including Drafting Recommendations)* [en línea]. Disponible en: <<http://www.adamsdrafting.com/downloads/Best-Efforts-Practical-Lawyer.pdf>>. [Fecha de consulta: 17 de enero de 2017].

ARMBRUST, Michael; FOX, Armando [et al]; *Above the Clouds: a Berkeley View of Cloud Computing* [en línea], 2009. Disponible en: <<http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html>>. [Fecha de consulta: 4 de julio de 2016].

BISWAS, Sourya; *Cloud Computing vs. Utility Computing vs. Grid Computing. Sorting the differences* [en línea], 2011. Disponible en: <<http://cloudtweaks.com/2011/02/cloud-computing-vs-utility-computing-vs-grid-computing-sorting-the-differences/>>. [Fecha de consulta: 6 de julio de 2016].

BRADSHAW, Simon; MILLARD, Christopher; WALDEN, IAN, "Standard contracts for Cloud Computing Services", *Cloud Computing Law*, 1ª edición, Oxford, 2013, págs. 37 a 72.

BORGHI, Maurizio; FERRETTI Federico; KARAPAPA, Stavroula, "Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK", *International Journal of Law and Information Technology*, Vol. 21, núm. 2, Oxford, 2013, págs. 109 a 153.

BROBERG, James; VENUGOPAL, Srikumar; BUYYA, Rajkumar; "Market-oriented Grids and Utility Computing: The State-of-the-art and Future Directions",

BIBLIOGRAFÍA

Journal of Grid Computing, Vol. 6, núm. 3, págs 255-276. BURRELL, Robert, COLEMAN, Alison; *Copyright exceptions: The Digital Impact*, 1ª edición, Cambridge, 2005, 460 págs.

CHANDRAKUMAR, T; PARTHASARATHY, S, "A framework for Evaluating Cloud Enterprise Resource Planning (ERP) Systems", *Continued Rise of the Clouds. Advances and Trends in Cloud Computing* (Ed. Zaigham Mahmood), Londres, 2014, págs. 161-175.

CHEN, Min; MAO, Shiwen, ZHANG, Yin; [et al.]; *Big Data Related Technologies, Challenges and Future Prospects*, 1ª edición, Nueva York, 2014, 104 págs.

CHENGA, Fa-Chang; LAIB, Wen-Hsing, "The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy, 2012 International Workshop on Information and Electronics Engineering", *Procedia Engineering*, Vol. 29, 2012, págs. 241 a 251.

CLAYBROOK, Bill, *Warning: Not All Cloud licensing Models Are user-Friendly* [en línea]. Disponible en: <<http://searchcloudcomputing.techtarget.com/feature/Warning-Not-all-cloud-licensing-models-are-user-friendly>>. [Fecha de consulta: 15 de agosto de 2016].

CLARKE, Roger; "Data risks in the Cloud", *Journal of Theoretical and Applied Electronic Commerce Research* [en línea], 2013. Disponible en: <<http://www.rogerclarke.com/II/DRC.html>>. [Fecha de consulta: 4 de julio de 2016].

COLSTON, Catherine; MIDDLETON; Kirsty; *Modern Intellectual Property Law*, 2ª edición, Londres, 2005, 808 págs.

CUNNINGHAM, Alan; REED, Chris, "Consumer Protection in Cloud Environments", *Cloud Computing Law* (Coord. Cristopher Millard), 1ª edición, Oxford, 2013, págs. 331 a 361.

CZARNY, Raphaël; "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: 9 de agosto de 2016].

DEL VECCHIO, José F; PATERNINA, Fabián; HENRÍQUEZ, Carlos; "Cloud Computing, a model for the development of enterprises", *Prospect*, Vol. 13, núm. 2,

BIBLIOGRAFÍA

81 a 87.

FAIRCHILD, Alea M.; "Patterns of Trust: Role of Certification for SME Cloud Adoption", *Continued Rise of the Cloud. Advances and Trends in Cloud Computing* (Coord: Zhaigham Maghmood), 1ª edición, Londres, 2014, págs. 145 a 158.

FERRANTE; Gabriele, "Italian contractual aspects of Cloud Computing", *Comparative Law Yearbook of International Business*, Vol. 37, 2015, págs. 127 a 147.

FISHMANN, Eric; CHARETTE, Aubrey; *Drafting a better "best efforts" clause* [en línea], 2013. Disponible en: <https://www.pillsburylaw.com/siteFiles/Publications/DraftingaBetterBestEffortsClause_CorporateCounsel072313.pdf>. [Fecha de consulta: 15 de agosto de 2016].

GEELAN, Jeremy, "Twenty-one Experts Define Cloud Computing" [en línea], *Cloud Computing Journal*, 2009. Disponible en: <<http://cloudcomputing.sys-con.com/node/612375>>. [Fecha de consulta: 24 de junio de 2016].

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: 8 de julio de 2016].

HESSELINK, M. W., "Towards a sharp distinction between b2b and b2c? On consumer, commercial and general law after the Consumer Rights Directive", *European Review of Private Law*, núm. 1, 2010, págs. 57 a 102.

HOLIDAY, Ryan; *How Facebook, Twitter and Other Startups Got Big* [en línea], 2014. Disponible en: <http://www.huffingtonpost.com/ryan-holiday/how-facebook-twitter-and-_b_4228942.html>. [Fecha de consulta: 28 de julio de 2016].

HON, W. Kuan; MILLARD, Christopher; "Negotiated contracts for Cloud Services", *Cloud Computing Law* (Ed. Christopher Millard), 1ª edición, Oxford, 2013, págs. 73 a 108.

HON, W. Kuan; MILLARD, Christopher; "Cloud Technologies and Services", *Cloud Computing Law* (Ed. Christopher Millard), 1ª edición, Oxford, 2013, págs 3 a 17.

HON, W. Kuan; MILLARD, Christopher; "Control, Security, and Risk in the Cloud", *Cloud Computing Law* (Ed. Christopher Millard), 1ª edición, Oxford, 2013, págs. 18-35.

BIBLIOGRAFÍA

HON, W. Kuan; MILLARD, C, "Cloud Computing vs Traditional Outsourcing. Key Differences" [en línea]. Disponible en: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200592>. [Fecha de consulta. 29 de febrero de 2016].

HUDSON, Thomas, *As-Is Sales: Buyer Beware? Or Dealer Beware?* [en línea], <<http://www.dealerbusinessjournal.com/articleview.php?id=651-58148>>. [Fecha de consulta: 17 de enero de 2017].

HURWITZ, Judith; KAUFMAN, Marcia; HALPER, Fern, *Cloud Services for Dummies. IBM Limited Edition*, 1ª edición, New Jersey, 2012, 64 págs.

HUSSEIN, Waaleed N.; SULAIMAN, Rosnafisah; "E-Business and Cloud Computing: A New Practice or a Trend", *Innovation in the High-Tech Economy* (Coord. Chuan Pang, *et. al.*), Berlín, 2013, págs. 67 a 77.

JACOB, Robin; ALEXANDER, Daniel; FISHER, Matthew; *Guidebook to Intellectual Property*, 6ª edición, Londres, 2013, 270 págs.

JANSEN, Dale; JANSEN, Cory, "What Clouds Middleware mean?", *Technopedia, the IT Education Site* [en línea]. Disponible en: <<https://www.techopedia.com/definition/30630/cloud-middleware-software>>. [Fecha de consulta: 17 de enero de 2017].

JANSEN, Dale; JANSEN, Cory, "What does Application Programming Interface mean?", *Technopedia, the IT Education Site* [en línea]. Disponible en: <<https://www.techopedia.com/definition/24407/application-programming-interface-api>>. [Fecha de consulta: 17 de enero de 2017].

JENNINGS, Eoin, *The Cloud is a commodity, or is it?* [en línea], 2013. Disponible en: <<http://cloud.verizon.com/cloud-blog/cloud-commodityor-it/>> [Fecha de consulta: 15 de enero de 2015].

JENSEN, Claus T.; *APIs and Intellectual Property* [en línea], 2015. Disponible en: <<https://developer.ibm.com/apimanagement/2015/02/16/apis-intellectual-property/>>. [Fecha de consulta: 15 de agosto de 2016].

JHAWAR, Ravi; PIURI, Vincenzo, "Fault Tolerance and Resilience in Cloud Computing Environments", *Computer and Information Security Handbook* (Coord. J. Vacca), 2ª edición, 2013, págs. 125 a 141.

KALPANA, P; LAHARIKA, M. "A comparative Study of Different

BIBLIOGRAFÍA

Deployment Models in a Cloud", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, 2013, págs. 512 a 515.

KAZELY, Harikleá; "Cloud Business Intelligence", *Business Information Systems Workshops. BIS 2014 International Workshops, Cyprus*, Suiza, 2014, págs. 307 a 317.

KLEYMAN, Bill; *Understanding Cloud APIs, and why they matter* [en línea], 2012. Disponible en: <<http://www.datacenterknowledge.com/archives/2012/10/16/understanding-cloud-integration-a-look-at-apis/>>. [Fecha de consulta: 15 de agosto de 2016].

MASNICK, Mike, *Why Making APIs Copyrightable Is Bad News for Innovation* [en línea], 2014. Disponible en: <<https://www.techdirt.com/articles/20140509/17140227184/why-making-apis-copyrightable-is-bad-news-innovation.shtml>>. [Fecha de consulta: 15 de agosto de 2016].

MELL, Peter; GRANCE, Timothy, "The NIST definition for Cloud Computing. Special Publication 800-145" [en línea], *National Institute of Standards and Technology, US Department of Commerce*, Gaithersburg, 2011. Disponible en: <<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>>. [Fecha de consulta: 17 de enero de 2017].

MYERSON, Judith; *Cloud Computing versus Grid Computing* [en línea], 2009. Disponible en: <<http://www.ibm.com/developerworks/library/wa-cloudgrid/>>. [Fecha de consulta: 7 de julio de 2016].

NOBLE FOSTER, T; "Navigating Through the Fog of Cloud Computing Contracts", *The John Marshall Journal of Information Technology & Privacy Law* [en línea], Vol. 30, 2013. Disponible en: <<http://repository.jmls.edu/cgi/viewcontent.cgi?article=1727&context=jitpl>>. [Fecha de consulta: 17 de enero de 2017].

NOUGRÈRES, Ana Brian, "La protección inteligente de los datos personales: Privacy by Design", *Revista Internacional de Protección de Datos Personales*, Universidad de los Andes, Colombia, núm. 1, 2012. Disponible en: <https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf>. [Fecha de consulta: 25 de mayo de 2016].

O'REILLY, Tom; "What is Web 2.0: Design Patterns and Business Models for

BIBLIOGRAFÍA

the next generation of Software", *Communications & Strategies*, núm. 65, 2007, págs. 17 a 37.

PARSI, Kalpana; LAHARIKA, M. "A comparative Study of Different Deployment Models in a Cloud" [en línea], *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, núm. 5, págs. 512 a 515. Disponible en: <http://www.ijarcse.com/docs/papers/Volume_3/5_May2013/V3I5-0229.pdf>. [Fecha de consulta: 24 de junio de 2016].

RAJ, Pethuru; "Enriching the Integration as a Service Paradigm for the Cloud Era", *Cloud Computing Principles and Paradigms* (Ed. Rajkumar Buyya, James Broberg, Andrzej Goscinski), 1ª edición, Nueva Jersey, 2011, págs. 57 a 96.

REED, Cris; CUNNINGHAM, Alan, "Ownership of Information in Clouds", *Cloud Computing Law* (Coord. Christopher Millard), 1ª edición, Oxford, 2013, págs. 142 a 164.

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: 24 de junio de 2016].

ROBERTS, Jeff John; *Supreme Court's API ruling puts the cloud over software industry* [en línea]. Disponible en: <<http://fortune.com/2015/06/29/supreme-court-oracle-api/>>. [Fecha de consulta: 15 de agosto de 2016].

ROGERS, Kathryn; *Oracle vs Google- Success for Oracle, JAVA APIs can have copyright protection* [en línea]. Disponible en: <<http://lawinthecloud.com/category/legal-issues/intellectual-property-rights/>>. [Fecha de consulta: 15 de agosto de 2016].

SCHAWISH, Ahmed; SALAMA, Maria; "Cloud Computing. Paradigms and Technologies", *Springer Studies in Computational Intelligence 495*, Berlín, 2014, págs. 39 a 67.

SCHMIDT, Rainer, MÖRING, Michael; MAIER, Stefan; PIETSCH, Julia; HÄRTING, Ralf-Cristian; "Big Data as Strategic Enabler -Insights from Central European Enterprises", *Business Information Systems: 17th International Conference, BIS 2014, Larnaca, Cyprus, May 22-23, 2014. Proceedings*, (Eds. Widock

BIBLIOGRAFÍA

Abramowitz, Angelika Kokkinaki), Suiza, 2014, págs 50 a 60.

SCHREIDER, Tari, "White Paper. The Legal Issues of Disaster Recovery Planning", *Disaster Recovery Journal* [en línea]. Disponible en: <<http://lbr.covalentwords.com/assets/docs/348.pdf>>. [Fecha de consulta: 17 de enero de 2017].

SIY, Sherwin; "Why You Can't Copyright an API" [en línea]. Disponible en: <<https://www.publicknowledge.org/news-blog/blogs/why-you-cant-copyright-an-api>>. [Fecha de consulta: 15 de agosto de 2016].

SMITH, Sonia; MAXWELL, Laurence; *The Sky is Not the Limit: Limitation of Liability Clauses May Be the Solution to Cap Your Contractual Liability* [en línea]. Disponible en: <<http://www.lorman.com/resources/the-sky-is-not-the-limit-limitation-of-liability-clauses-may-be-the-solution-to-cap-your-contractual-liability-15452>>. [Fecha de consulta: 17 de enero de 2017].

SPINELLO, Richard A; TAVANI, Herman; *Intellectual Property Rights in a Networked World*, 1ª edición, Londres, 2005, 300 págs.

STIENINGER; Mark; NEDBAL, Dietmar; "Drivers for the Actual Usage of Cloud Services: An Examination of Influencing Factors for Digital Natives", *Human-Computer Interaction. Applications and Services*. Suiza, 2014, págs. 69 a 79.

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.

VOORSLUYS, William; BROBERG, James; BUYYA, Rajkumar, "Introduction to Cloud Computing", *Cloud Computing Principles and Paradigms* (Coord. Rajkumar Buyya, James Broberg, Andrzej Goscinski), 1ª edición, Nueva Jersey, 2011, págs. 3 a 43.

WAEDELDE, Charlotte; LAURIE, Graeme (et el.); *Contemporary Intellectual Property Law and Policy*, 3ª edición, Londres, 2014, 1104 págs.

WINKLER, Matteo M; MOSCA, Jacopo, "Cloud Computing e Protezioni dei dati personali" (coord. M. Fumagalli Meraviglia), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, Nápoles, 2015, págs. 12 a 140.

WINKLER, Vic; *Cloud Computing Legal and Regulatory issues* [en línea], 2012. Disponible en: <<http://technet.microsoft.com/en->

BIBLIOGRAFÍA

us/magazine/hh994647.aspx>. [Fecha de consulta: 15 de agosto de 2016].

WIPO, *Intellectual Property Handbook* [en línea]. Disponible en: <http://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf>. [Fecha de consulta: 15 de agosto de 2016].

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].

ZHANG, Qi; CHENG, Lu; BOUTABA, Raouf. "Cloud computing: state-of-the-art and research challenges" [en línea], *Brazilian Computer Society*, 2010, págs. 7 a 18. Disponible en: <<http://link.springer.com/article/10.1007%2Fs13174-010-0007-6>>. [Fecha de consulta: 6 de julio de 2016].

ZHAO, Liang [et al.]; *Cloud Data Management*, 1ª edición, Suiza, 2014, 202 págs.

Guías, informes, recomendaciones, estudios socio-económicos, estándares técnicos, noticias en prensa y otros documentos

ABANLEX, "Informe sobre la obligación legal de notificar o denunciar brechas de seguridad que afecten a datos personales" [en línea]. Disponible en: <https://www.abanlex.com/wp-content/Arbor/Informe_sobre_obligaciones_de_notificar_y_denunciar.pdf>. [Fecha de consulta: 24 de mayo de 2017].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía del Reglamento General de Protección de Datos para responsables de tratamiento* [en línea]. Disponible en: <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf>. [Fecha de consulta: 15 de mayo de 2017].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *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: 17 de enero de 2017].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Orientaciones para*

BIBLIOGRAFÍA

prestadores de servicios de Cloud Computing [en línea]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf>. [Fecha de consulta: 24 de mayo de 2017].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía de seguridad de datos* [en línea]. Disponible en: <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf>. [Fecha de consulta: 17 de enero de 2017].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *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: 17 de enero de 2017].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía modelo del documento de seguridad* [en línea]. Disponible en: <https://www.agpd.es/portalwebAGPD/canalresponsable/guia_documento/index-ides-idphp.php>. [Fecha de consulta: 17 de enero de 2017].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD), *Plan de inspección de oficio a cadenas hoteleras* [en línea], 2004. Disponible en: <<https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/RECOMENDACIONESCADENASHOTELERASDEFINITIVAS.pdf>>. [Fecha de consulta: 24 de marzo de 2017].

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN AENOR. *UNE 71380/2014*. Disponible en: <<http://www.iso27000.es/sgsi.html#seccion1>>. [Fecha de consulta: 17 de enero de 2017].

AVANADE, *Rethink application possibilities and align to desired business outcomes* [en línea], 2013. Disponible en: <http://www.avanade.com/advisor/application-development/Documents/AppDev_VBResearch_Whitepaper_GLOBAL.pdf>. [Fecha de consulta: 27 de junio de 2016].

BBVA OBSERVATORIO DE ECONOMÍA DIGITAL, *El desarrollo de la industria del Cloud Computing: impactos y transformaciones en marcha* [en línea], 2014. Disponible en: <<https://www.bbvaesearch.com/publicaciones/el-desarrollo-de-la-industria-del-cloud-computing-impactos-y-transformaciones-en-marcha/>>.

BIBLIOGRAFÍA

[Fecha de consulta: 24 de mayo de 2017].

BUREAU EUROPEÉN DES UNIONS DE CONSOMMATEURS (BEUC), *Unfair Contract Terms in Cloud Computing Service Contracts Discussion Paper* [en línea]. Disponible en: <http://www.beuc.eu/publications/beuc-x-2014-034_are_ec_expert_group_on_cloud_computing_contracts.pdf> [Fecha de consulta: 27 de abril de 2016].

CISCO, *Global Cloud Index: Forecast and Methodology. 2014-2019 Whitepaper* [en línea], 2016. Disponible en: <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/Cloud_Index_White_Paper.html>. [Fecha de consulta: 4 de julio de 2016].

CLOUD COMPUTING STRATEGY, *Discussion Papers* [en línea]. Disponibles en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 24 de mayo de 2017].

CLOUD INDUSTRY FORUM, *Code of Practice for Cloud Computing Providers* [en línea]. Disponible en: <<http://cloudindustryforum.org/code-of-practice/code-of-practice>>. [Fecha de consulta: 15 de enero de 2015].

CLOUD SECURITY ALLIANCE CSA, *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1* [en línea], 2009. Disponible en: <<https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf>>. [Fecha de consulta: 27 de junio de 2016].

CLOUD SECURITY ALLIANCE CSA, *Top threats in Cloud Computing, V1* [en línea], 2010. Disponible en: <<https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>>. [Fecha de consulta: 27 de junio de 2016].

CLOUD STANDARDS CUSTOMER COUNCIL, Cloud Computing Use Case Discussion Group, *Cloud Computing Use Cases White Paper v. 4.0* [en línea], 2010. Disponible en: <http://www.cloud-council.org/Cloud_Computing_Use_Cases_Whitepaper-4_0.pdf>. [Fecha de consulta: 27 de noviembre de 2015]

CLOUD STANDARDS CUSTOMER COUNCIL "*Practical Guide to Cloud Service Agreements Version 2.0*", [en línea]. Disponible en: <http://www.cloud-council.org/CSCC_Practical_Guide_to_Cloud_Service_Agreements_Version_2.0.pdf>. [Fecha de consulta: 24 de mayo de 2017].

BIBLIOGRAFÍA

CLOUD STANDARDS CUSTOMER COUNCIL, "*Public Cloud Service Agreements: What to Expect and What to Negotiate*" [en línea], 2013. Disponible en: <<http://www.cloud-council.org/PublicCloudServiceAgreements2.pdf>>. [Fecha de consulta: 3 de diciembre de 2015].

CLOUD STANDARDS CUSTOMER COUNCIL, *Interoperability and Portability for Cloud Computing. A guide* [en línea], 2014. Disponible en: <<http://www.cloud-council.org/deliverables/CSCC-Interoperability-and-Portability-for-Cloud-Computing-A-Guide.pdf>>. [Fecha de consulta: 22 de febrero de 2017].

CLOUD STANDARDS CUSTOMER COUNCIL, "*Security for Cloud Computing. Ten Steps to Ensure Success*", 2015 [en línea]. Disponible en: <<http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf>>. [Fecha de consulta: 28 de noviembre de 2016].

COMISIÓN EUROPEA. *Agenda Digital de la Cloud Computing Strategy*. Disponible en: <<http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy>>. [Fecha de consulta: 24 de mayo de 2017].

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: 12 de julio de 2016].

COMISIÓN EUROPEA Comunicación de la Comisión Europea al Parlamento Europeo, al Consejo, Al Comité Económico y Social y al Comité de las Regiones COM (2012) 529 final, "*the potential of Cloud Computing in Europe*" [en línea]. Disponible en: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF>>. [Fecha de consulta: 12 de julio de 2016].

COMISIÓN EUROPEA, *Cloud Service Level Agreement Standardisation Guidelines* [en línea]. Disponible en: <<https://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines>> [Fecha de consulta: 14 de noviembre de 2016].

COMISIÓN EUROPEA, *Cloud Contracts Expert Group (Cloud Computing Strategy) Discussion papers* [en línea]. Disponibles en: <http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm>. [Fecha de consulta: 14 de noviembre de 2016].

BIBLIOGRAFÍA

COMISIÓN EUROPEA, *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una Estrategia para el Mercado Único Digital de Europa, COM (2015) 192 final* [en línea]. Disponible en: <<http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52015DC0192&from=EN>>. [Fecha de consulta: 15 de diciembre de 2016].

COMISIÓN EUROPEA, Dirección General de Redes de Comunicación, Contenidos y Tecnología, Unidad E2, Software y Servicios *Cloud*, "Cloud Computing Service Level Agreements. Exploitation of Research Results" [en línea], 2013. Disponible en: <<https://ec.europa.eu/digital-single-market/en/news/cloud-computing-service-level-agreements-exploitation-research-results>>. [Fecha de consulta: 24 de mayo de 2017].

EFOR, *Informe sobre la realidad tecnológica de las empresas en Aragón* [en línea], 2014. Disponible en: <<http://www.efor.es/sites/default/files/informe-cios-aragon.pdf>>. [Fecha de consulta: 4 de julio de 2016].

ENISA, *Cloud Security Guide for SMEs* [en línea], 2015. Disponible en: <<https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/security-for-smes/cloud-security-guide-for-smes>>. [Fecha de consulta: 27 de junio de 2016].

ENISA, *Computación en nube. Beneficios, riesgos y recomendaciones para la seguridad de la información* [en línea], 2009. Disponible en: <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment-spanish/at_download/file>. [Fecha de consulta: 27 de junio de 2016].

ETSI, *Cloud Standards Coordination Final Report, november 2013, version 1.0* [en línea]. Disponible en: <http://csc.etsi.org/resources/CSC-Phase-1/CSC-Deliverable-008-Final_Report-V1_0.pdf>. [Fecha de consulta: 17 de enero de 2017].

EXCELTUR, *Estudio de Impacto Económico del Turismo sobre la Economía y el Empleo de las Islas Baleares, IMPACTUR 2014* [en línea]. Disponible en: <<http://www.exceltur.org/impactur/>>. [Fecha de consulta: 3 de abril de 2017].

FORO TURISMO.AS; SOCIEDAD ESTATAL PARA LA GESTIÓN DE LA INNOVACIÓN Y LAS TECNOLOGÍAS TURÍSTICAS (SEGITTUR), "ThinkTank *Cloud Computing y Turismo*" [en línea], 2012. Disponible en:

BIBLIOGRAFÍA

<<http://www.segittur.es/opencms/export/sites/segitur/.content/galerias/descargas/notas-prensa/Informe-conclusiones-Think-Tank-Cloud-Computing-y-Turismo.pdf>>. [Fecha de consulta: 27 de febrero de 2017].

FUNDACIÓN DE LA INNOVACIÓN BANKINTER, *Cloud Computing, La tercera ola de las tecnologías de la información* [en línea], 2010. Disponible en: <<https://www.accenture.com/es-es/insight-cloud-computing-summary>>. [Fecha de consulta: 4 de julio de 2016].

FUNDACIÓN ORANGE, *España: La transformación digital en el sector turístico* [en línea], 2016. Disponible en: <http://www.fundacionorange.es/wp-content/uploads/2016/05/eE_La_transformacion_digital_del_sector_turistico.pdf>. [Fecha de consulta: 17 de marzo de 2017].

FUNDACIÓN TELEFÓNICA, *Desarrollo Empresarial y Redes Sociales. El caso de las microempresas españolas* [en línea], 2015. Disponible en: <http://www.fundaciontelefonica.com/arte_cultura/publicaciones-listado/pagina-item-publicaciones/itempubli/331/>. [Fecha de consulta: 17 de marzo de 2017].

GARTNER Inc., *Gartner's Magic Quadrant for Cloud Infrastructure as a Service*, 2014 [en línea]. Disponible en <<http://www.gartner.com/technology/reprints.do?id=1-1UKQQA6&ct=140528&st=sb>>. [Fecha de consulta: 28 de mayo de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre el derecho a la portabilidad de los datos* [en línea], 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].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Directrices sobre los delegados de protección de datos* (GT 243), 2016 [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].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing* (WP 232), [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf>. [Fecha de consulta: 15 de septiembre de 2017].

BIBLIOGRAFÍA

2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 5/2014 sobre técnicas de anonimización* (WP 216) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf>. [Fecha de consulta: 15 de septiembre de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Opinión 03/2014 sobre la notificación de violación de datos personales* (WP 213) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_es.pdf>. [Fecha de consulta: 15 de septiembre de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 05/2012 sobre Cloud Computing* [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf>. [Fecha de consulta: 27 de junio de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Opinión 15/2011 sobre definición del consentimiento* (WP 187) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_es.pdf>. [Fecha de consulta: 27 de junio de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 8/2010 sobre Ley aplicable* (WP 179) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_es.pdf>. [Fecha de consulta: 15 de septiembre de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *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/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_es.pdf>. [Fecha de consulta: 15 de septiembre de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 5/2009 sobre las redes sociales en línea* (WP 163) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf>.

BIBLIOGRAFÍA

[recommendation/files/2009/wp163_es.pdf](#)>. [Fecha de consulta: 15 de septiembre de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 4/2007 sobre el concepto de datos personales* (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: 15 de septiembre de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Documento de Trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE* (WP 56) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp56_es.pdf>. [Fecha de consulta: 15 de septiembre de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Opinión 4/2000 sobre el nivel de protección que proporcionan los principios de puerto seguro* (WP 32) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp32_es.pdf>. [Fecha de consulta: 15 de septiembre de 2016].

GRUPO DE TRABAJO DEL ARTÍCULO 29, *Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE* (WP 12) [en línea]. Disponible en: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_es.pdf>. [Fecha de consulta: 15 de septiembre de 2016].

HOSTELTUR, *Priceline compra la startup española Hotel Ninjas*. Disponible en: <https://www.hosteltur.com/159150_priceline-compra-start-up-espanola-hotel-ninjas.html>. Fecha de consulta: 17 de marzo de 2017].

HOTREC, *"Benchmarks of Fair Practices in Online Distribution"* [en línea]. Disponible en: <<http://www.hotrec.eu>>. [Fecha de consulta: 23 de marzo de 2017].

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:

BIBLIOGRAFÍA

<<https://ec.europa.eu/digital-agenda/en/news/final-report-study-smart-20130043-uptake-cloud-europe>>. [Fecha de consulta: 27 de junio de 2016].

IDC, *Construir una Cloud híbrida: la TI como servicio* [en línea], 2015. Disponible en: <<http://www.acens.com/blog/wp-content/images/construir-cloud-hibrida-idc-emc-informe-blog-acens-cloud.pdf>>. [Fecha de consulta: 24 de junio de 2016].

IDC, *Estudio especial Cloud en España 2013: Hacia un nuevo Cloud* [en línea], 2014. Disponible en: <http://www.eventosidc.es/Estudio_Especial/Cloud_en_Espana.php>. [Fecha de consulta: 27 de junio de 2016].

IDC, *Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake* [en línea], 2012. Disponible en: <<http://ec.europa.eu/digital-agenda/en/news/quantitative-estimates-demand-cloud-computing-europe-and-likely-barriers-take-final-report>>. [Fecha de consulta: 27 de junio de 2016].

INSTITUTO NACIONAL DE CIBERSEGURIDAD INCIBE (anteriormente denominado INTECO), *Nueve claves de ciberseguridad para el sector del Turismo* [en línea], 2016. Disponible en: <<https://www.incibe.es/protege-tu-empresa/blog/9-claves-ciberseguridad-el-sector-del-turismo>>. [Fecha de consulta: 21 de marzo de 2017].

INSTITUTO NACIONAL DE CIBERSEGURIDAD INCIBE (anteriormente denominado INTECO), *Guía para empresas: seguridad y privacidad del Cloud Computing* [en línea]. Disponible en: <https://www.incibe.es/CERT/guias_estudios/guias/Guia_Cloud>. [Fecha de consulta: 15 de septiembre de 2016].

INTECO (Instituto Nacional de Ciberseguridad, antes INTECO), *Guía para empresas: identidad digital y reputación online* [en línea], 2012. Disponible en: <http://empresasyemprendedores.aytosalamanca.es/es/downloads/guia_identidad_reputacion_empresas_final_nov2012x1x.pdf>. [Fecha de consulta: 21 de marzo de 2017].

INSTITUTO NACIONAL DE CIBERSEGURIDAD INCIBE (anteriormente denominado INTECO), *Riesgos y Amenazas en Cloud Computing* [en línea], 2011. Disponible en

BIBLIOGRAFÍA

<http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_r iesgos_y_amenazas_en_cloud_computing.pdf>. [Fecha de consulta: 27 de junio de 2016].

INSTITUTO NACIONAL DE CIBERSEGURIDAD INCIBE (anteriormente denominado 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>. [Fecha de consulta: 27 de junio de 2016].

INSTITUTO NACIONAL DE ESTADÍSTICA INE, *Retrato de la PYME a 1 de enero de 2016* [en línea]. Disponible en: <<http://www.ipyme.org/publicaciones/retrato-pyme-dirce-1-enero-2016.pdf>>. [Fecha de consulta: 23 de marzo de 2017].

INSTITUTO NACIONAL DE ESTADÍSTICA INE, *Retrato de la PYME 2015* [en línea], 2015. Disponible en: <http://www.ipyme.org/publicaciones/retrato_pyme_2015.pdf>. [Fecha de consulta: 27 de junio de 2016].

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: 28 de junio de 2016].

KPMG, *Cloud Takes Shape* [en línea], 2013. Disponible en: <<http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/cloud-service-providers-survey/Documents/the-cloud-takes-shapev2.pdf>>. [Fecha de consulta: 27 de junio de 2016].

INCIBE (Instituto Nacional de Ciberseguridad, anteriormente denominado INTECO), *Guía para empresas: seguridad y privacidad del Cloud Computing*, [en línea]. Disponible en: <https://www.incibe.es/CERT/guias_estudios/guias/Guia_Cloud>. [Fecha de consulta: 29 de septiembre de 2015].

INCIBE, "*Guía sobre almacenamiento y borrado seguro de información*", 2011 [En línea]. <https://www.incibe.es/CERT/guias_estudios/guias/guia_borrado_seguro>. [Fecha de consulta: 20 de febrero de 2017].

BIBLIOGRAFÍA

LONDON ECONOMICS, *Study on the Economic Benefits of Privacy Enhancing Technologies – Final Report to the European Commission DG Justice, Freedom, and Security* [en línea], 2010. Disponible en: <http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf>. [Fecha de consulta: 15 de septiembre de 2016].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST; *Special publication 1500-1. Big Data Interoperability Framework: Volume 1: Definitions* [en línea], 2015. Disponible en: <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-1.pdf>>. [Fecha de consulta: 27 de junio de 2016].

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: 7 de julio de 2016].

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST; *Special Publication 800-144. Guidelines on Security and Privacy in Public Cloud Computing* [en línea], 2011. Disponible en: <<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf>>. [Fecha de consulta: 27 de junio de 2016].

OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y LOS SISTEMAS DE INFORMACIÓN (ONTSI), *La sociedad en Red. Informe Anual 2015. edición 2016*, [en línea]. 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].

OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y LA SOCIEDAD DE LA INFORMACIÓN ONTSI, *Informe e-Pyme 2016. Análisis sectorial de la implantación de las TIC en la PYME española* [en línea]. Disponible en: <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: 27 de febrero de 2017]

ONTSI; FUNDETEC; *Informe ePYME 2015. Análisis sectorial de la*

BIBLIOGRAFÍA

implantación de las TIC en la PYME española [en línea], 2015. Disponible en: <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: 27 de junio de 2016].

ONTSI; FUNDETEC; *Informe ePYME 2014. Análisis sectorial de la implantación de las TIC en la PYME española* [en línea], 2014. Disponible en: <<http://www.ipyme.org/Publicaciones/informe-epyme-2014.pdf>>. [Fecha de consulta: 27 de junio de 2016].

OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y LOS SISTEMAS DE INFORMACIÓN (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>>. [Fecha de consulta: 27 de junio de 2016].

PÉREZ, David; *Startups 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].

PENTEIO, *Cloud Computing en la empresa española 2013* [en línea], 2013. Disponible en: <<http://www.revistacloudcomputing.com/wp-content/uploads/2013/06/resumen-informe-penteo-cloud-computing-2013.pdf>>. [Fecha de consulta: 27 de junio de 2016].

PWC ESPAÑA; *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.pdf>>. [Fecha de consulta: 27 de junio de 2016].

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: 2 de agosto de 2016].

RUBIC, Dado, *Facebook supera los 1280 millones de usuarios activos* [en línea], Reuters, 23 de abril de 2014. Disponible en:

BIBLIOGRAFÍA

<http://cincodias.com/cincodias/2014/04/23/tecnologia/1398284063_477857.html>. [Fecha de consulta: 24 de abril de 2017].

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].

SOFTDOIT, *Las herramientas de marketing y ventas y el uso del CRM en las empresas españolas en 2016* [en línea], 2017. Disponible en: <<https://www.softwaredoit.es/estudio/estudio-herramientas-marketing-ventas-uso-software-crm-empresas-espana-2016.html>>. [Fecha de consulta: 6 de marzo de 2017].

TECNOHOTEL, *Hotel Ninjas se alía con Salesforce para ampliar sus servicios en la nube*. Disponible en: <<https://www.tecnohotelnews.com/2016/07/infografia-mas-del-50-de-las-empresas-espanolas-tienen-alojadas-sus-soluciones-crm-en-la-nube/>>. [Fecha de consulta: 13 de marzo de 2017].

THE ECONOMIST, *Cloud computing. A market for computing power* [en línea], 2011. Disponible en: <<http://www.economist.com/node/18185752>>. [Fecha de consulta: 2 de agosto de 2016].

YANGUAS GÓMEZ, Roberto, "Modification of the contracts" [en línea], *European Commission, Expert Group on Cloud Computing Contracts Discussion Paper*. Disponible en: <http://ec.europa.eu/justice/contract/files/expert_groups/modification_contracts_en.pdf>. [Fecha de consulta: 20 de febrero de 2017].

Webgrafía

Amicus Brief Computer Scientist, in Support of Petition of Writ of Certiorari. [Fecha de consulta: 15 de agosto de 2016]. Disponible en: <<https://www.eff.org/document/amicus-brief-computer-scientists-scotus>>.

Business Cloud News. Disponible en: <<http://www.businesscloudnews.com/>>. [Fecha de consulta: 15 de agosto de 2016]

Cloud Industry Forum. Disponible en: <<http://www.cloudindustryforum.org>>

BIBLIOGRAFÍA

[Fecha de consulta: 27 de junio de 2016].

Cloud Standards Wiki. Disponible en: <http://cloud-standards.org/wiki/index.php?title=Main_Page>. [Fecha de consulta: 6 de julio de 2016].

Creative Commons. Disponible en: <<http://es.creativecommons.org/blog/cc-es/>>. [Fecha de consulta: 15 de agosto de 2016].

EMC2, glosario EMC: *Nube privada*. Disponible en: <<http://spain.emc.com/corporate/glossary/private-cloud.htm>>. [Fecha de consulta: 27 de junio de 2016].

Estándar ISO /IEC 20000-1:2011 [En línea], <http://www.iso.org/iso/catalogue_detail?csnumber=51986>. [Fecha de consulta: 7 de diciembre de 2015].

Estándar ISO /IEC 17788:2014 [En línea], <http://www.iso.org/iso/catalogue_detail?csnumber=60544>. [Fecha de consulta: 14 de noviembre de 2016].

Estándar ISO/IEC 27017 [En línea]. Disponible en: <<http://www.iso27001security.com/html/27017.html>>. [Fecha de consulta: 28 de diciembre de 2016].

Free Software Foundation. Disponible en: <<https://www.fsf.org>>. [Fecha de consulta: 15 de agosto de 2016].

Fundéu BBVA. Disponible en: <<http://www.fundeu.es/recomendacion/cloud-computing-prefierase-computacion-en-nube-540>>. [Fecha de consulta: 27 de junio de 2016].

Gen beta. Disponible en: <<http://www.genbetadev.com/actualidad/google-maps-la-api-deja-de-ser-gratuita>>. [Fecha de consulta: 15 de agosto de 2016].

GNU. Disponible en: <<http://www.gnu.org/licenses/license-list.html#SoftwareLicenses>>. [Fecha de consulta: 15 de agosto de 2016].

INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS (IEEE), "*IEEE Standard Definitions for Use in Reporting Electric Generating Unit Reliability, Availability and Productivity*" [en línea], 2006. Disponible en: <<http://www.nerc.com/docs/pc/gadstf/ieee762tf/762-2006.pdf>>.

BIBLIOGRAFÍA

OMPI Organización Mundial de la Propiedad Intelectual. Disponible en: <<http://www.wipo.int>>. [Fecha de consulta: 15 de agosto de 2016].

Open Cloud Consortium. Disponible en: <<http://opencloudconsortium.org/about/>>. [Fecha de consulta: 15 de agosto de 2016].

Search for Extra-Terrestrial Intelligence SETI. Disponible en <<http://setiathome.ssl.berkeley.edu/>>. [Fecha de consulta: 30 de marzo de 2017].

TAR Certification, [en línea]. Disponible en: <<https://resilience.enisa.europa.eu/cloud-computing-certification>>. [Fecha de consulta: 13 de septiembre de 2014].

Techtarget. Disponible en: <<http://searchcloudcomputing.techtarget.com/definition/cloud-bursting>>. [Fecha de consulta: 27 de junio de 2016]

Términos y condiciones. Disponible en: <<http://terminosycondiciones.es/>> [Fecha de consulta: 15 de agosto de 2016].

Terms of Service Didn't Read. Disponible en: <<https://tosdr.org/>>. [Fecha de consulta: 15 de agosto de 2016].

Términos y condiciones consultados

ACENS

Condiciones Generales de Contratación Electrónica

ADRIVE

Adrive Terms of Service

AMAZON

Amazon Web Services S3 (Simple Storage Services)

Amazon Drive

BOOKING

Términos y Condiciones de Booking

BOX

Box Terms of Use

BIBLIOGRAFÍA

CLARANET

Condiciones Generales de los Servicios Claranet

Condiciones Particulares de los Servicios de Hosting

Condiciones Particulares de los Servicios de Gestión

*Condiciones Particulares de los Servicios de Virtual Data Center
(VDC)*

Política de Privacidad

DROPBOX

Dropbox Para Empresas

Dropbox Para Particulares

ELASTIC HOST

Elastic Host Cloud Servers

ENGISOFT

Condiciones Generales

Política de Privacidad

FACEBOOK

*Declaración de derechos y responsabilidades (Condiciones del servicio
de Facebook)*

Política de Datos

Normas de la Comunidad de Facebook

GOOGLE

Condiciones Generales para servicios de Google

Google App Engine

Google Compute Engine

Google G-Suite (anteriormente, Google Apps For Bussiness).

Google Cloud Platform

INSTAGRAM

BIBLIOGRAFÍA

Condiciones de uso de Instagram

Política de Privacidad

Normas de la Comunidad de Instagram

LA CASA DEL LIBRO

Condiciones Generales de Contratación

Política de Protección de Datos

MARKETMAN

MarketMan Terms of Use

MICROSOFT

Condiciones Generales para servicios de Microsoft

Microsoft Dynamics CRM

Microsoft Dynamics NAV 2016

Microsoft Office 365

Microsoft OneDrive

MINUBE

Términos de Uso y Contratación & Política de Privacidad

MOVISTAR

Servidor Cloud de Movistar

ODOO

Odoo Apps Terms and Conditions 7.0

ORACLE-

Oracle Cloud Rightnow

RASTREATOR.COM

Aviso Legal

SALESFORCE

Force.com Free Edition Agreement

SAP

BIBLIOGRAFÍA

SAP Hana Cloud Developer

SUITECH

Política de Privacidad

TRIPADVISOR

Condiciones de Uso

Términos y Condiciones de PerfilPlus de TripAdvisor

Política de Privacidad

Política de Cookies

TRIVAGO

Términos y Condiciones de Trivago

Política de Privacidad

Política de Cookies

Información Legal

TWITTER

Términos de Uso

Política de Privacidad

UKFAST

Terms and Conditions

Code of Practice

Cloud Service Level Agreement

VODAFONE

Políticas de Uso de Comunicaciones Electrónicas para particulares y autónomos