CLOUD COMPUTING: ASPECTOS JURÍDICOS CLAVE PARA LA CONTRATACIÓN DE ESTOS SERVICIOS

Rafael García del Poyo[*]

RESUMEN

En este artículo se analiza cómo se debe estructurar y diseñar la contratación empresarial de los servicios de Cloud Computing, a la luz de la normativa española y europea, atendiendo a los aspectos más relevantes de estos servicios y facilitando las claves para cubrir los riesgos jurídicos que pueden surgir durante la fase de contratación de estos servicios y en la fase de prestación de los mismos.

***Palabras Clave*:** Cloud Computing.

1. DEFINICIÓN DEL CLOUD COMPUTING. ELEMENTOS CARACTERIZADORES.

El "cloud computing" es un nuevo modelo de negocios a través del cual, mediante la utilización de tecnologías de la información y de las comunicaciones, se posibilita a los usuarios la capacidad de acceder a un catálogo de servicios estandarizados que sirven para

[*] Abogado. Socio responsable del sector de Digital Business. Osborne Clarke.

responder a las necesidades de los individuos y de las empresas de una forma flexible y adaptativa.

Desde el punto de vista tecnológico el Cloud Computing puede definirse como un "paradigma de programación" que permite ofrecer servicios informáticos a través de Internet. El término Cloud o nube, es obviamente una alusión metafórica a Internet.

Mediante este sistema los clientes pueden acceder a determinados servicios que se encuentran almacenados de forma permanente en servidores remotos y cuando un cliente así lo solicita, se hace inmediatamente disponible en sus equipos de escritorio, centros de ocio, dispositivos portátiles, etc. según las necesidades requeridas de cada momento de forma que el cloud computing se ha constituido como un auténtico "modelo a la carta" para la prestación de servicios relacionados con el software, las aplicaciones y las infraestructuras tecnológicas.

Los servicios que se prestan por medio del Cloud Computing se basan en tres características esenciales que deben ser contempladas cuando se configuren los contratos de Cloud Computing para que contemplen los riesgos jurídicos que estos conllevan.

- Multiposesión: El esquema de funcionamiento del cloud computing se basa en información que es almacenada de manera permanente en servidores o data centers, accesibles a través de Internet, pero esta comunicación con los servidores no se realiza de forma única por un solo cliente, de modo que los mismos son compartidos por multitud de usuarios en un modelo de multiposesión (multi tenancy) de modo que multitud de personas pueden utilizarlos de forma concurrente.

    - El acceso a los servicios on line de manera personalizada: El cliente para acceder a los servicios prestados a través del cloud computing basta con que tenga una adecuada infraestructura de telecomunicaciones que le facilite acceso a Internet, no se precisa instalación de ningún software adicional, ya que -habitualmente- suelen usarse browsers o buscadores para acceder a todos los servicios ofrecidos en Cloud. Esta circunstancia da lugar a que el modelo Cloud resulte en una mayor compatibilidad y capacidad de integración con el resto de aplicaciones informáticas que también poseen las empresas clientes. El cliente se puede abastecer unilateralmente de capacidades de

procesamiento, tiempo de utilización de servidor, capacidad de almacenamiento en red, etc. según las necesidades empresariales de cada momento, de una forma rápida y elástica (incluso, en algunos casos, de forma automática) y sin que se requiera la interacción humana con el proveedor de servicios.

- Optimización y control de recursos de forma bilateral: Los sistemas informáticos disponibles mediante Cloud Computing controlan y optimizan el uso de los recursos de manera automática. El uso de estos recursos por parte de los clientes puede seguirse, controlarse y notificarse, lo que aporta una enorme transparencia en la gestión del negocio para ambas partes.

Estas características implican la necesidad que los contratos de cloud computing contemplen estas realidades mediante acuerdos pormenorizados que por un lado contemplen los niveles de prestación del servicio con modelos precisos para la gestión de información, pautas de aislamiento, segmentación de sus datos en relación con terceros teniendo en cuenta que los servicios se prestan bajo un esquema de multiposesion, sin olvidar que el contrato también debe reflejar todas las funcionalidades que permite obtener la nube como son el , abastecimiento de capacidades de procesamiento, de almacenamiento, de tiempo de utilización del servicio de manera aleatoria etc …

A lo largo del siguiente capítulo vamos a estudiar en qué consisten la nube que tipos de nube existen y que tipos de servicios se pueden ofrecer así como sus beneficios y riesgos para finalmente abordar qué tipo de contratos se deben realizar cuando se realiza la contratación de estos servicios y las cláusulas que deben obligatoriamente contemplar para una adecuada protección jurídica ambas partes.

2. MODELOS DE "NUBES"

Existen cuatro formas fundamentales de prestación de los servicios en la nube en función del control y de la gestión de los entornos informáticos, lo cual, como después veremos más adelante, tiene una importancia fundamental a la hora de dotarle de la necesaria cobertura jurídica.

En este sentido podemos distinguir las denominadas:

a.) **"Nubes públicas"** que son gestionadas por empresas prestadoras de estos servicios y en las que se atienden a una pluralidad de clientes (bien el público en general, bien un grupo industrial, etc.) mediante la utilización de servidores, sistemas de almacenamiento y otras infraestructuras que se utilizan de forma compartida.

b.) **"Nubes privadas"** son aquellas infraestructuras manejadas en favor de un solo cliente el cual suele decidir los usuarios que quedan autorizados a utilizar la infraestructura y que controla las aplicaciones, los servidores, etc. Puede gestionarla la propia organización cliente o un tercero y puede residir tanto en las instalaciones del cliente como fuera de ellas. Este tipo de nubes suelen implantarse para la gestión de sistemas informáticos que necesitan un alto grado de sincronización o que trabajan con bases de datos que involucran un considerable grado de complejidad.

c.) **"Nubes comunitarias"** son aquellas en las que la infraestructura tecnológica se comparte entre diversas organizaciones que mantienen objetivos similares, por ejemplo, en materia de requisitos de seguridad, o sobre consideraciones relacionadas con el cumplimiento normativo. Puede ser gestionada por las propias organizaciones o por un tercero y puede establecerse en las propias instalaciones de la comunidad o grupo o fuera de ellas.

d.) **"Nubes híbridas"** son aquellas que combinan elementos definitorios de los modelos de nubes públicas, comunitarias y privadas, por lo que los clientes pueden ser propietarios de unas partes y compartir otras con otros clientes aunque de una manera controlada. En este caso, la infraestructura de nube suele basarse en tecnología estandarizada o propietaria que permite la portabilidad de datos y de aplicaciones. Este tipo de nubes suelen ser las utilizadas en el caso de empresas que necesite una infraestructura tecnológica simple, que no requiera un alto grado de sofisticación pero que a su vez pueda ser escalable en capacidad en un corto espacio de tiempo.

3. TIPOS DE SERVICIOS

En ocasiones, el Cloud Computing se confunde con los denominados sistemas informáticos de "grid" (o en red) que son más bien sistemas a través de los cuales un "superordenador virtual" compuesto por un conjunto enlazado de ordenadores actúa de manera concertada para realizar tareas que requieren una gran capacidad de procesamiento.

En este sentido, conviene destacar que la diferencia fundamental que aporta el Cloud Computing a los modelos de negocio radica en la posibilidad de aumentar de forma gradual y escalable el número de servicios prestados a través de Internet. Esto genera beneficios tanto para los proveedores, que pueden ofrecer, de forma más rápida y eficiente, un mayor número de servicios, como para los usuarios o clientes lo cuales tienen la posibilidad de acceder a ellos, disfrutando de la sencillez e inmediatez del sistema y, potencialmente, de un modelo de pago por consumo.

Existen tres modelos fundamentales que junto a sus combinaciones derivadas describen los tipos de prestación de los servicios que cabe realizar a través de la nube. Habitualmente, y de manera genérica, se hace referencia a esos tres modelos fundamentales como el "Modelo SPI," donde "SPI" hace referencia a Software, Plataforma e Infraestructura (as a Service, o como Servicio), respectivamente, y se definen del siguiente modo:

a.) Software como Servicio (SaaS)

El SaaS se caracteriza por la puesta a disposición de un software ofrecido como un servicio bajo demanda que se utiliza de forma compartida con otros usuarios, lo cual implica que un solo software que reside en la infraestructura del proveedor del servicio puede ser utilizado por múltiples organizaciones empresariales o clientes. Su antecesor fue el denominado ASP (Application Service Provider).

b.) Plataforma como Servicio (PaaS)

Se trata de plataformas de desarrollo de software como herramienta de desarrollo a la cual se accede a través de Internet. De esta forma, los desarrolladores pueden construir nuevas aplicaciones sin tener que instalar ninguna herramienta específica en sus propios ordenadores, por lo que se hace posible el acceso a esa herramienta sin necesidad de tener conocimientos especializados. En estas plataformas, la ventaja que se proporciona al cliente, básicamente, consiste en poner a su disposición lenguajes y herramientas de programación que son gestionadas por el prestador de servicios.

c.) Infraestructura como Servicio (IaaS)

Tiene como principal característica el servir como medio para alcanzar capacidad tanto de procesamiento informático como de almacenamiento de información a través de servicios estandarizados prestados a través de Internet de forma que el cliente puede desplegar y ejecutar software de cualquier tipo, ya sean sistemas operativos o software específico.

4. BENEFICIOS Y RIESGOS

Las ventajas que ofrece la nube son muchas, el hecho de que la empresa -en principio- no va a verse en la necesidad de instalar ningún hardware adicional y, por lo tanto, se requerirá de una inversión inicial menor de la que debería haberse realizado en el pasado para obtener unos rendimientos productivos similares, se producen mayores compatibilidades y capacidades de integración con el resto de aplicaciones informáticas, proporcionando una mayor capacidad de recuperación en caso de desastre y reduciendo los tiempos de inactividad del sistema. Otra de las grandes ventajas de la nubes es que se permite en paralelo por parte del cliente un seguimiento continuo de su actividad, lo que contribuye a realizar una gestión transparente que repercute en un mayor "bienestar contractual" de las partes.

Si bien es cierto que la contratación de servicios en la nube entraña ciertos riesgos y límites dentro de la gestión de la empresa, algunos aducen que limita la libertad de gestión de las empresas clientes y las hace excesivamente dependientes de su proveedor de servicios y, a su vez, ello redunda en que se limita tanto la libertad como la creatividad de la empresa cliente para estructurar y organizar de una cierta manera su información.

El grupo de trabajo del artículo 29 en su opinión 05/2012 ha advertido acerca de los riesgos para la confidencialidad, disponibilidad, integridad, y portabilidad de los datos, ya que a través del cloud computing se pone en peligro la libertad de disposición de la información de las empresas, argumento este especialmente digno de consideración si aceptamos que en la sociedad de la información el activo más valioso de una compañía es precisamente su información.

En este sentido el grupo de trabajo advierte acerca de los siguientes riesgos fundamentales[1]:

- Disminución de disponibilidad debido a la merma en la interoperabilidad (cautivos de un sólo proveedor): Si un cliente contrata exclusivamente con una solo proveedor de servicios en la nube que le garantiza un servicio completo puede ser complicado transferir datos y documentos entre diferentes sistemas de proveedores de nubes (data portability) o intercambiar información con otras entidades que utilizan un sistema diferente de nubes (interoperabilidad)

- Disminución de la integridad de los sistemas por operar con recursos compartidos: Las infraestructuras de las nubes se realizan a través de sistemas y recursos compartidos. De forma que los datos personales de personas físicas u organizaciones estén dentro de infraestructuras de seguridad más complicadas.

- Disminución de confidencialidad: Es el riesgo que entraña que los servidores donde se aloje la información de la nube no se encuentren dentro del ámbito territorial de la UE y por lo tanto no cumplan con la normativa de seguridad que exige la UE en materia de protección de datos.

[1] Opinion 5/2012 emitidael 1 de Julio de 2012 por el grupo de trabajo del artículo 29.

- Disminución de la capacidad de control debido a la complejidad de las dinámicas de la externalización de los servicios: Los proveedores de servicios de nube suelen utilizar a su vez otros proveedores que pueden cambiar a lo largo del contrato, dificultando el control sobre los mismos y pudiendo provocar cambios durante la prestación del servicio.

De este modo se advierte que mediante el funcionamiento del modelo cloud las compañías depositan sus informaciones de negocio más valiosas y los datos personales de los que disponen en manos de terceros, y esta información recorre diferentes nodos para llegar a su destino, cada uno de ellos y sus respectivos canales de acceso pueden convertirse en un foco permanente de inseguridad y por esta razón, se deben utilizar protocolos seguros. Otro riesgo reside en la velocidad de acceso a la información que puede llegar a disminuir drásticamente, debido a la sobrecarga que requieren este tipo de protocolos lo cual puede llegar a producir un excesivo grado de dependencia tanto de los proveedores de servicios de cloud computing como de los proveedores de acceso a Internet, o que la externalización de los servicios cloud puede implicar que la información acabe alojándose en países que no pertenecen a la Unión Europea sin las garantías que esta exige en materia de protección de datos.

Finalmente, si nos centramos exclusivamente en los proveedores de servicios altamente especializados, la prestación completa de los servicios al cliente que los solicita puede llegar a tardar meses o incluso años. Y, por otro lado, si tenemos en cuenta que la madurez funcional de las aplicaciones informáticas hace que continuamente deban incorporarse modificaciones, puede ocurrir que, para aquellas empresas cliente de baja intensidad en la utilización de recursos tecnológicos, la curva de aprendizaje puede alcanzar un exiguo rendimiento.

5. CONCIENCIACIÓN

El empresario que dados todos los riesgos que se están poniendo de manifiesto considere finalmente recibir servicios a través del modelo cloud deberá asegurarse que la de que la seguridad de su información en esos entornos debe tratarse de igual manera que el resto de las "cuestiones críticas de seguridad en su cadena de suministro".

Por ello, en el cloud computing cobran especial relevancia los potenciales riesgos jurídicos que hacen referencia a la identificación e implementación contractual de las estructuras, procesos y controles organizativos adecuados necesarios para gestionar la seguridad de la información (como un elemento más del proceso productivo) y alcanzar un cumplimiento normativo efectivo.

Como punto de partida, las empresas deben ser muy conscientes de que trasladar información, datos y aplicaciones informáticas a un esquema de prestación de servicios en la nube repercute muy directamente en las políticas y en los procedimientos internos de la empresa cliente.

Por tanto, las empresas deberán evaluar qué políticas y procedimientos están dispuestos a modificar y a cambiar de forma íntegra. Algunos ejemplos de las políticas y procedimientos que pueden verse afectados y cuya regulación debe preverse en el clausulado del contrato que regule la prestación de servicios bajo el régimen de cloud computing son los informes de actividad, las políticas de retención de datos, los procedimientos de respuesta a incidencias, la normativa de las auditorías de control interno y externo y las políticas de privacidad de la compañía.

No debemos olvidar que el cloud computing implica la presencia de una empresa tercera -el proveedor de servicios en la nube- y que ésta va a tener acceso a la organización empresarial y a la información que se gestiona, lo que va a dar lugar a nuevos retos a la hora de determinar las leyes y los contratos que se aplican a la gestión de la información.

Conviene también recordar que mucha de la legislación relacionada con la informática que las empresas deben cumplir no se redactó pensando en el cloud computing y, a modo de ejemplo, es muy posible que los auditores u otros asesores

externos con los que habitualmente colabora la empresa no estén familiarizados con el cloud computing en general o con algún servicio en la nube en particular.

En todo caso, corresponde al cliente de los servicios de cloud computing comprender cuáles son las exigencias de cumplimiento normativo que implica la prestación de un determinado servicio a través del modelo nube, procurar un reparto equitativo entre el proveedor de la nube y su cliente de las nuevas responsabilidades de cumplimiento normativo. Por ello, resulta evidente la conveniencia de establecer unas condiciones adecuadas de nivel de calidad del servicio prestado por la empresa de Cloud contratada (generalmente detalladas en los denominados SLAs –por sus siglas en inglés correspondientes al término Service Level Agreement-), así como contemplar las dificultades que pudieran surgir del proceso de migración a los servicios de Cloud junto a otras muchas cuestiones que podrán surgir relacionadas con la privacidad y confidencialidad de la información.

Los departamentos jurídicos y de tecnología de las empresas clientes deberán implicarse y trabajar "codo con codo" durante el establecimiento de los Contratos de Nivel de Servicios y de las obligaciones contractuales, al objeto de garantizar qué requisitos de seguridad se pueden solicitar y alcanzar contractualmente mediante el establecimiento de métricas y estándares adecuados.

6. CLOUD COMPUTING B2B

La frecuencia con la que los beneficiarios de servicios tecnológicos de prácticamente todos los sectores se embarcan en esquemas de Cloud presenta en los últimos años un grado de crecimiento vertiginoso, más aún cuanta mayor conciencia y publicidad adquieren las compañías de las ventajas que esta forma de prestación de servicios les puede reportar.

La contratación de los servicios Cloud se realiza a todos los niveles tanto como por parte de personas físicas en calidad de consumidores, como por parte de las

Administraciones debido a las obligaciones que se le impusieron a través de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los ciudadanos a los Servicios Públicos, por la que entre otras las administraciones debían mejorar las gestiones de procesos, siendo el modelo cloud una alternativa económica y viable para mejorar los servicios públicos y finalmente entre personas jurídicas encuadrados dentro de la típica contratación mercantil,

Cada tipo de contratación dependiendo de las partes implica condiciones muy diferentes de las mismas ya que por ejemplo en los supuestos de contratación de servicios de Cloud B2C el consumidor , por lo general, habrá de adherirse a unas Condiciones Generales de Contratación establecidas por la empresa prestadora de los servicios de Cloud, en cambio en el marco de una relación B2B para la prestación de estos servicios, será el prestador de servicios de Cloud el que –normalmente- deba amoldarse en cada caso a las necesidades específicas de su cliente.

Es decir, mientras que el "poder de mercado" en el ámbito minorista lo tiene claramente el prestador de servicios de Cloud (obviando la capacidad de influir en su conducta competitiva que puedan tener los consumidores como colectivo), en el ámbito estrictamente empresarial será el cliente el que tenga la capacidad –dentro siempre de los límites que marca toda negociación contractual- de establecer las características que requiere y espera de una prestación de servicios de este tipo.

En este artículo se analizará la prestación de servicios entre empresas de las relaciones denominadas B2B (Business to Business, en inglés), esto es, entre contratación mercantil entre empresas Este aspecto, una de cuyas traducciones puede resultar en el denominado común consentimiento, se complementa, en términos de elementos caracterizadores del contrato, con el hecho de que el mismo resulta en el nacimiento de una serie de obligaciones, así como que adquiere fuerza de ley entre las partes.

7. EL CONTRATO DE PRESTACIÓN DE SERVICIOS DE CLOUD

7.1 El carácter mercantil de los contratos empresariales de Cloud

Como ya avanzamos en el epígrafe anterior, la prestación de servicios de Cloud a empresas se articula a través de un elemento básico y fundamental: la firma de un contrato entre las partes.

Si bien es cierto en nuestro ordenamiento jurídico no se regula expresamente la materia del cloud computing, no es menos cierto que –a nuestro juicio-tanto el derecho español como la legislación europea[2] aportan una respuesta general y suficiente a los interrogantes de carácter normativo que se plantean en la operativa diaria de este modelo. De ahí que surja la necesidad de regular este tipo de actividades por vía contractual, con independencia de que ello sea o no una práctica lo suficientemente habitual.

El encuadramiento de este tipo de contratos dentro de una u otra clase vendrá determinado exclusivamente por la normativa que le fuera de aplicación, sin que el dotarle de un nombre concreto tenga mayor relevancia. Normalmente, los contratos utilizados para regular los servicios de cloud computing suelen ser contratos de adhesión en los que los proveedores de servicios en la nube imponen sus propias condiciones (a pesar de que lo más deseable sería que fuesen contratos específicamente negociados entre las partes) con el consiguiente riesgo para la parte contratante ya que no posee capacidad de negociación respecto del reparto de responsabilidad en la seguridad de la conservación de los contenidos, la obligatoriedad del cumplimiento en materia de datos etc…

En todo caso debería regir el ya mencionado principio de libertad de forma, contenido en el artículo 51 del Código de Comercio y en los artículos 1278 y siguientes

[2] En materia normativa en su opinión 5/2012 del grupo de trabajo del artículo 29 emitida el 1 de julio de 2012, ha manifestado que la normativa aplicable en este ámbito son las Directivas 95/46/EC en materia de protección de datos y la Directiva sobre la privacidad de las comunicaciones electrónicas-
En este sentido los criterios que se deben tomar en cuenta para la legislación aplicable a estos contratos son los que se determinan en el art. 4 de la Directiva 95/46/EC, que es aplicable para los proveedores de servicios que poseen mas de un establecimiento en el Espacio Económico Europeo (EEA) o para los que no lo posean pero se sirvan de equipos localizados dentro del EEA. Así el factor que determinará la ley aplicable será el lugar el lugar desde donde el cliente sea el receptor de los servicios obviándose de este modo el lugar desde donde el proveedor de servicios opere o el tipo de nube que este utilizando.

del Código Civil, conforme al cual las partes podrán contratar sin que los acuerdos alcanzados hayan de dotarse de unas características formales concretas. En todo caso, y al encontrarnos en un supuesto de contratación B2B, sí podemos afirmar que el supuesto que aquí analizamos constituye un contrato de tipo mercantil. El que un contrato empresarial de prestación de servicios de Cloud se repute mercantil tiene como fundamento el hecho de que el objeto del mismo lo constituye un acto de comercio de los regulados en el Código de Comercio. Adicionalmente a lo anterior, el hecho de que la contratación se produzca entre empresas en el ámbito de su negocio, supone una nota más para la determinación del carácter mercantil de estos contratos. La regulación de este tipo de contratos, por tanto, vendrá determinada por las disposiciones del Código de Comercio y, supletoriamente, por lo establecido en materia de contratos en el Código Civil.

Podría, de otro lado, optarse por una clasificación de este tipo de contratos en virtud del negocio jurídico que los mismos vienen a regular. Así, venimos hasta aquí refiriéndonos a contratos de prestación de servicios, si bien conviene aclarar que los mismos, en numerosas ocasiones, se configuran como generadores de obligaciones de medios y no de resultados. Esto es, el prestador queda comprometido a procurar una serie de facilidades, siendo éste el objeto del contrato, sin que le resulten exigibles resultados satisfactorios. Sin embargo, no es éste el supuesto al que nos enfrentamos, pues dada la relevancia de las funcionalidades que la empresa interesada en la contratación estaría delegando y pretendiendo del prestador de servicios de Cloud, deviene en todo caso fundamental establecer una serie de compromisos de resultado. Así, cabría apellidar a nuestro contrato de prestación de servicios con el término «externalización», aunque más generalmente encontraremos el empleo del término inglés «outsourcing». El concepto de externalización de los servicios no ofrece dudas respecto de su significado e implicaciones, sin embargo, no está de más acudir a la definición concreta que de la expresión «outsourcing informático» hace M. Á. Davara[3] Rodríguez, y conforme a la cual el mismo consiste en:

«(…) *la cesión de la gestión de los sistemas de información de una entidad a un tercero que, especializado en esta área, se integra en la toma de decisiones y desarrollo*

[3] DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. Manual de Derecho Informático. 10ª Edición. Thomson Aranzadi, Madrid, 2008, p. 278.

de las aplicaciones y actividades propias de la referida gestión, con la finalidad de la optimización de los resultados de la misma, al tiempo que permite a la entidad el acceso a nuevas tecnologías y la utilización de recursos especializados de los que no dispone».

Si bien tal definición parece exceder el ámbito de los contratos de Cloud, por incluir no sólo el almacenamiento de datos e información (que es en lo que realmente consistiría el Cloud en sentido estricto) sino también la gestión de esa misma información mediante aplicaciones tecnológicas concretas, lo cierto es que la realidad nos demuestra la frecuencia con la que el objeto de estos contratos supera el mero almacenamiento de información. Así, adicionalmente al ahorro de espacio y a las facilidades de organización de los datos de una empresa, las compañías beneficiarias de los servicios de Cloud buscan una reducción significativa de costes a través de la externalización no solo de los contenidos sino de su gestión, con la pretensión final tanto de reducir costes estructurales como de optimizar los recursos de la propia empresa.

Así pues, conviniendo que nos encontramos ante un contrato de prestación de servicios de outsourcing ejecutado a través de un esquema o paradigma de Cloud, podemos afirmar sin lugar a dudas que el mismo constituye un contrato de los denominados atípicos, por carecer de regulación específica, al menos, en la legislación española. De este modo, le resultará de aplicación de manera supletoria la normativa que con carácter general regula las obligaciones y contratos (nuevamente, el Código Civil en sus artículos 1088 a 1314 en todo aquello no cubierto por el Código de Comercio), así como toda aquella normativa que por razón del objeto de la compañía afecte al desempeño de la sociedad.

7.2 Normativa aplicable a los contratos empresariales de Cloud

Sin perjuicio de lo anterior, y como consecuencia de los distintos ámbitos afectados por el contenido del contrato, por razón del tipo de servicios que se prestan, y el sector de actividad en que quedan enmarcados los mismos, encontramos que la normativa que resulta de aplicación no se limita a la estrictamente mercantil y, por extensión civil, sino que habrá de tomarse en consideración un amplio espectro de normas

sectoriales específicas. En este sentido y lógicamente, conviene aquí dejar presente que la aplicación de las disposiciones normativas a las que van a hacerse alusión dependerá de forma determinante de si la ley aplicable al contrato de prestación de servicios en Cloud resulta ser la española. De cualquier modo, si la legislación española no resultase de aplicación al contrato deberá encontrarse y reflejarse en el contrato la normativa homóloga que venga a regular las situaciones que se nos presentan. Sirva este capítulo, al menos, para ayudar al lector a identificar aquellos aspectos jurídicos que cobran una mayor relevancia a la hora de establecer un contrato, de forma que puedan éstos regular con el mayor detalle posible todos aquellos aspectos esenciales que deben ser abordados en este contexto.

A este respecto, y dentro del marco normativo español, no podemos dejar de citar ciertas normas que ya han sido abordadas en distintos capítulos de la presente obra, pues si bien se ha procedido ya o se procederá más adelante a analizarlas con detenimiento, no dejan de ser relevantes a la hora de elaborar un contrato empresarial de servicios de Cloud. De entre todas ellas, destaca la normativa de protección de datos de carácter personal (en concreto, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal –LOPD- y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD), pues los servicios de Cloud, en la inmensa mayoría de los casos, implican un flujo constante de información (entre la que se encuentran los datos de carácter personal) que deberá quedar convenientemente cubierto desde el punto de vista contractual según lo previsto en la normativa española. De otro lado, el hecho de que los servicios de Cloud inevitablemente se presten en el marco de la denominada Sociedad de la Información, hará que se deba prestar también especial atención a lo dispuesto en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico –LSSI-, en especial cuando los servicios en cuestión puedan suponer la posibilidad de formalizar contratos por vía electrónica; asimismo, el prestador de servicios de Cloud quedará obligado por la LSSI como prestador que es de servicios de la Sociedad de la Información, viéndose incluso sometido a un régimen sancionador específico. No es menos relevante la normativa de propiedad intelectual (y concretamente el Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), pues deberán las partes tener en cuenta que el empleo de

aplicaciones, programas informáticos, e incluso contenidos involucrados en la prestación de servicios de Cloud pueden –suelen- ser objeto de protección específica dado su carácter de obras.

Por descontado, un considerable número de disposiciones de distinta naturaleza habrán de ser tenidas en cuenta en la configuración de la relación contractual que vinculará a las partes, incluso aunque su incidencia sobre la misma sea indirecta: entre otras, disposiciones fiscales, laborales e incluso de carácter constitucional.

8. CLÁUSULAS TÍPICAS DE UN CONTRATO EMPRESARIAL DE SERVICIOS DE CLOUD

8.1 El contrato marco y sus anexos

El contrato empresarial de servicios de Cloud se estructura generalmente en torno a dos partes fundamentales: de un lado, el propio contrato -denominado en muchas ocasiones contrato marco- que contendrá los aspectos de carácter general que regularán la relación entre las partes, y de otro, los anexos –o adendas- que complementan a aquél con el detalle y las especificaciones particulares que asegurarán la conveniencia y satisfacción de las necesidades de la empresa contratante.

El hecho de que la práctica más habitual pase por esta división no persigue sino simplificar la comprensión y organización del propio contrato. Así, los anexos deben contener aquellas consideraciones que resulten eminentemente técnicas sin que ello suponga que su contenido sea de importancia inferior a lo estipulado en el propio contrato marco. Más bien al contrario, con frecuencia se encuentra que el detalle del alcance de los servicios que deben ser prestados por la empresa de Cloud queda contenida en un anexo, así como incluso el propio precio pactado (e incluso las condiciones de facturación) entre las partes y generalmente desglosado en correlación con cada una de las prestaciones pactadas.

Es también habitual acompañar como anexo al contrato el detalle de los procedimientos a seguir para los servicios de operación y mantenimiento a llevar a cabo por el prestador de servicios de Cloud; este anexo, suele incluir, además, un reparto de responsabilidades entre las partes en el que queda establecido a cuál de ellas corresponde la obligación de contratar determinados servicios de terceros: desde los servicios de un call center hasta la contratación de una plataforma de pago online. De otro lado, y en relación con las cuestiones relacionadas con protección de datos de carácter personal ya vistas, el detalle correspondiente a las medidas de seguridad a adoptar en cumplimiento de la normativa vigente al respecto suele constituir otro de los anexos típicos de los contratos de prestación de servicios de Cloud.

Por último, y sin perjuicio de la aproximación que más adelante en el presente capítulo se hará al efecto, uno de los principales anexos lo constituyen los denominados Acuerdos de Nivel de Servicio (o SLAs: "Service Level Agreements" en inglés), mediante los que se plasman las obligaciones mínimas de calidad, disponibilidad y continuidad en la prestación del servicio. Igualmente, las responsabilidades por incumplimiento del Acuerdo de Nivel de Servicio, esto es, las penalizaciones que se derivan de la inobservancia de las condiciones establecidas en dicho Acuerdo, pueden quedar incluidas en el mismo anexo o en uno separado.

En definitiva, si bien los aspectos fundamentales para la configuración y validez de la relación establecida entre las partes se asienta sobre las cláusulas típicas que conforman el contrato marco, los anexos constituyen un complemento esencial para que la materialización de las prestaciones acordadas resulte satisfactoria para ambas partes. Por esta razón, resulta muy aconsejable que desde un punto de vista eminentemente práctico, y debido a la constante evolución de las funcionalidades que procuran las tecnologías de la información y de las comunicaciones, en el contrato marco se establezcan aquellos mecanismos procedimentales que procuren que los anexos "técnicos" puedan renovarse durante toda la vigencia del contrato siempre que concurran el consentimiento de ambas partes y el de las personas designadas en cada parte, sin que el contrato marco deba ser también modificado.

8.2 Las cláusulas típicas

8.2.1 Identificación de las partes, expositivos, el objeto del contrato

Tal y como se adelantaba ya en el subapartado anterior, el contrato marco o, si se prefiere, el cuerpo mismo del contrato empresarial de servicios de Cloud contendrá los aspectos principales mediante los que se dará forma a la relación contractual que vinculará a las partes. Por supuesto, el contrato de prestación de servicios de Cloud comenzará con la necesaria identificación de los contratantes, donde se hará constar, no solo la identidad de los mismos y de sus representantes (representación que deberá quedar debidamente acreditada mediante la identificación de los instrumentos de apoderamiento, sin que resulte excesiva una declaración de vigencia de los mismos por parte del firmante a la fecha de suscripción del contrato), sino también la actividad a la que cada una de las empresas se dedican.

La costumbre -pues como se ha dicho rige en los contratos el principio de libertad de forma- nos indica que seguidamente a la identificación de los contratantes encontraremos por lo general la denominada parte expositiva. En la misma, se enumeran con cierto nivel de detalle (sin que sea necesaria ni conveniente una pormenorización excesiva, más propia de otras jurisdicciones) las necesidades de una de las partes –aquella que será beneficiaria de los servicios de Cloud- y las posibilidades de satisfacer las mismas de que dispone la otra parte, el prestador de los servicios de Cloud. Resulta igualmente conveniente incorporar expositivos claros pero concisos sobre las necesidades, razones e intenciones que llevan a las partes a formalizar el contrato en cuestión y que, ante el potencial surgimiento de discrepancias en la interpretación de las cláusulas subsiguientes podrán resultar de utilidad por arrojar cierta luz respecto de la intención verdadera de los contratantes. Tal y como resume M. Á. Davara:[4]

[4] DAVARA RODRÍGUEZ, MIGUEL ÁNGEL. *Manual de Derecho Informático.* 10ª Edición. Thomson Aranzadi, Madrid, 2008, p. 286.

«(…) *es de interés establecer claramente el negocio jurídico en el cual luego, de acuerdo con la teoría general para ese negocio en el ordenamiento, se pueda subsumir el caso e interpretar el contrato*».

Las partes, expuestas sus intenciones, acuerdan mediante una declaración la firma del contrato en cuestión, cuyas condiciones habrán de sostenerse sobre la base de las cláusulas que, por lo general, acompañan a continuación a los expositivos ya vistos. De entre tales cláusulas –y conviene aquí una vez más hacer referencia al principio de libertad de forma- existe una serie de ellas típicas, por recurrentes y fundamentales en la estructuración y conformación de las condiciones contratadas. De entre ellas, fundamental nuevamente es la relativa al objeto del contrato, pues la misma colaborará a la correcta resolución de posibles controversias interpretativas y supondrá una contextualización del resto de cláusulas.

8.2.2 Las obligaciones de las partes

Quizá una de las cláusulas de mayor relevancia sea aquella encaminada a determinar las obligaciones de cada una de las partes nacidas de la formalización del contrato (generalmente dividida en dos subcláusulas contenedoras de las obligaciones de cada una de las partes respectivamente). La identificación de los elementos con los que cada una de las obligaciones de cada respectiva parte tiene relación resulta fundamental, pues la omisión de alguno de ellos en particular –así como de alguna de las obligaciones en general- podría dar lugar a una responsabilidad falta de adjudicación, lo cual sin duda constituirá un claro germen de conflicto entre las partes.

La conveniencia de que las obligaciones de las partes y la correcta asignación de las mismas se realicen con especial atención a la claridad de su redacción no resulta baladí. Y ello, precisamente por la misma razón apuntada con anterioridad: en la búsqueda de evitar conflictos de interpretación o de exigencias de responsabilidades por incumplimiento de las obligaciones contractuales.

En este sentido debe mencionarse que existe la posibilidad de que los propios proveedores de servicios externalicen parte de sus servicios a través de contratos de outsourcing y es importante que si esto ocurre se asegure y se identifique la cadena de responsabilidad a lo largo de los procesos y servicios para tener un control efectivo sobre los servicios que van a ser prestados.

La normativa europea no prohíbe que se realicen este tipo de acuerdos entre los proveedores de servicios de cloud computing, pero que en todo caso la otra parte debe conocer que habrá ciertos procesos que estarán externalizados. El grupo de discusión del artículo 29 manifiesta en su opinión 5/2012 de 1 de julio, que en el caso de que existan empresas subcontratadas para la externalización de los servicios, el deber del proveedor de servicios es informar desde el primer momento y por escrito a la otra parte de la existencia de los mismos, así como identificarlos. Asimismo incide en que con el fin de evitar vacíos de responsabilidad por daños causados por estas empresas subcontratadas es conveniente que se añadan cláusulas en los contratos de modo que los prestadores de servicios Cloud con los que se contrata se responsabilicen de la actuación y cumplimiento de la normativa de las empresas subcontratadas.

En el contexto de la prestación de servicios de Cloud, ya las obligaciones de las partes (en caso de que no se hubiera hecho previamente en la cláusula determinante del objeto del contrato), y concretamente las que atañen al prestador de los servicios, podría darnos una idea del tipo de servicios de Cloud que regula el contrato en cuestión. Así, podría establecerse, incluso ya con claridad, si los servicios a prestar consistirían en un modelo de Cloud tipo SaaS (Software as a Service), PaaS (Platform as a Service) o IaaS (Infrastructure as a Service, conforme a las definiciones de los mismos vistas en capítulos anteriores, en función, claro está, de hasta dónde alcancen las obligaciones asumidas por el prestador de servicios de Cloud. No obsta decir, a este respecto, que el beneficiario de los servicios de Cloud deberá asegurarse de que el alcance de los servicios contratados, y por ende las obligaciones que deberá asumir el prestador, habrán de hacerse constar debidamente en esta cláusula de forma que se satisfagan adecuadamente las necesidades que pretende cubrir mediante la formalización de este contrato.

En el cloud computing existe un sentido de[5] "independencia de la ubicación física sobre la que el propio cliente generalmente no tiene control, lo cual suele traducirse en que desconoce el lugar exacto en el que se encuentran los servidores a través de los cuales se obtienen los recursos contratados. Sin embargo, se puede (y se debe) pedir al prestador de servicios que contractualmente aporte informaciones específicas sobre el país, la región, o un determinado centro de datos, así como sobre su capacidad para realizar una potencial asignación adicional de recursos humanos y materiales -en caso de que se hiciese necesaria- en relación con la capacidad de almacenamiento y procesamiento de información, las redes de telecomunicación que procura acceso a la misma, o con la disposición de máquinas virtuales.

De hecho, resulta muy conveniente prever contractualmente las consecuencias que deben derivarse de la posibilidad de que, en la medida en que un mayor número de clientes compartan la infraestructura de la nube, se produzcan sobrecargas en los servidores y degradaciones en la calidad del servicio efectivamente ejecutado por los prestadores.

Las empresas clientes deben reservarse en todo caso la capacidad de auditar al proveedor de servicios en la nube, habida cuenta de la naturaleza dinámica tanto del entorno tecnológico de Internet como del ámbito normativo. Como decimos, los clientes deben incluir en los contratos la posibilidad de auditar, en el marco de un adecuado proceso de due diligence, las infraestructuras informáticas y los procesos de gestión de la seguridad de la información implantados por el proveedor.

Definitivamente, la cláusula contractual referente a la reserva del derecho a auditar debe obtenerse siempre que sea posible, muy especialmente cuando se utiliza un proveedor en la nube para un servicio ante el cual el cliente mantiene importantes responsabilidades de cumplimiento normativo. A lo largo del tiempo, la necesidad del ejercicio de este derecho debería reducirse y sustituirse por las adecuadas certificaciones estándar de un proveedor de servicios en la nube.

El contrato debe permitir al cliente de los servicios en la nube o a quien se designe, realizar el seguimiento del rendimiento de los proveedores de servicio y de comprobar las vulnerabilidades del sistema informático del que se dispone. Tampoco

[5] Ver nota número 2 acerca de la normativa europea en este aspecto.

debe descartarse la conveniencia de planificar la resolución tanto esperada como inesperada de la relación en las negociaciones contractuales, y una devolución metódica o enajenación segura de tus activos. En todo caso, el proveedor de servicios en la nube y el cliente deberían disponer de un proceso unificado para responder a citaciones, emplazamientos y otras solicitudes legales

Adicionalmente, y pese a que ello podría deducirse del contenido genérico del contrato, no tiene por qué ser excesivo el establecer con claridad si las obligaciones a las que quedan sujetas cada una de las partes son obligaciones de medio u obligaciones de resultado. Conviene enfatizar que los contratos empresariales de prestación de servicios de outsourcing de Cloud pueden llegar a generar en el prestador de los mismos obligaciones de resultado y no simplemente de medio. Tales obligaciones de resultado deben quedar debidamente delimitadas y abordadas mediante los Acuerdos de Nivel de Servicio de los que más adelante nos ocuparemos.

8.2.3. Protección de datos de carácter personal

La relevancia que cobra este aspecto en los contratos empresariales de servicios de Cloud genera, como consecuencia, que deba siempre incluirse una cláusula que contemple la regulación contractual de la protección de datos de carácter personal.

Sin perjuicio del modo en que se articule el flujo de datos en cada caso particular, por lo general, una prestación de servicios de Cloud entre empresas supondrá un supuesto de comunicación de datos a un tercero conforme a lo recogido en el artículo 11.2.c de la LOPD. Sin embargo, como decimos, dependiendo de cada caso concreto, podría incluso tratarse de un encargo de tratamiento de datos personales recogido en el artículo 12 del mismo texto normativo.

En cualquier caso, y sea cual fuere el supuesto, la cláusula deberá identificar claramente al responsable del fichero de datos en cuestión, así como en su caso quién actuará como encargado de su tratamiento. Por otra parte, y como se verá, las partes pueden incluir –y generalmente se configura como anexo- un detalle de las medidas de

seguridad a adoptar de conformidad con lo establecido en el Reglamento de desarrollo de la LOPD.

La pérdida de control directo sobre tal información comporta en todo caso un riesgo, cuya cobertura debe preverse en el ámbito contractual, y particularmente mediante la negociación y acuerdo de las condiciones en que se vaya a prestar el servicio de cloud computing (sin perjuicio, por supuesto, de la conveniencia de que la contratación de estos servicios se lleve a cabo con empresas del sector de reconocido prestigio, a ser posible sin manchas en su historial de infracciones relativas a la seguridad de la información tratada).

Conviene por lo tanto establecer un cláusula por la que se establecerán las condiciones en que el tratamiento de los datos tendrá lugar y la finalidad para la que se destinarán los mismos. Del mismo modo, deviene fundamental asegurarse de que el prestador de servicios de Cloud pondrá en funcionamiento las medidas de seguridad necesarias para proteger el acceso a los datos en cuestión; medidas de índole técnica y organizativa que deberán garantizar la seguridad e integridad de los datos, impidiendo su alteración, pérdida, tratamiento o acceso no autorizado y siendo en todo caso acordes con la naturaleza de los datos.

Esta información de la empresa, sobre la que de alguna manera pierde el control directo, implica la entrega de la misma a un tercero, pudiendo ser los datos compartidos de distinto tipo en virtud del alcance o las funcionalidades Cloud contratadas. Así, podemos encontrarnos tanto ante una transferencia de datos de carácter personal (a modo de ejemplo, datos de los empleados transmitidos para la prestación de un servicio de recursos humanos o de elaboración de nóminas) como ante información constitutiva de secreto comercial de la compañía. Así, las medidas a adoptar para su protección variarán en función del tipo de información que se comparte con el prestador de servicios.

Conviene igualmente tener presente que este tipo de servicios se prestan a menudo valiéndose de un traslado de la información por parte del prestador a servidores que pudieran estar ubicados en el extranjero. He aquí, pues, otro aspecto altamente relevante que debe evaluarse en la forma adecuada en el momento de negociación del contrato de servicios de Cloud pues, en función de las condiciones en que tal movimiento internacional de datos se produzca, las implicaciones para las partes son muy diversas, y

pueden llegar a exigir la autorización del Director de la Agencia de Protección de Datos (AEPD), o, en su caso, la notificación a la AEPD de tal transferencia de datos.

La normativa aplicable y, por extensión, la AEPD en su manera de proceder, persiguen, mediante la limitación o imposición de condiciones a estas transferencias de carácter internacional, el aseguramiento de una protección de los datos de carácter personal con un "nivel equiparable" al establecido en la LOPD. En estas circunstancias, en aquellos casos en que la transferencia tenga como destino un Estado Miembro de la Unión Europea, o un Estado respecto del cual la Comisión de Europea, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado, no será necesaria la expresa autorización del Director de la AEPD (sin perjuicio de la notificación preceptiva a la misma por la cual se ponga en su conocimiento que se va a producir una transferencia internacional de datos).

Por lo tanto, la importancia de conocer dónde tiene previsto ubicar los datos el prestador de servicios de Cloud no es -ni mucho menos- poco relevante. Y ello, no sólo por cuanto la notificación o autorización de la AEPD pudiera resultar preceptiva, sino también para poder realizar un análisis de la confianza que el país en el que se alojarán los datos transmita a la compañía, así como para obtener una mayor garantía de que las medidas de seguridad implantadas para proteger sus datos serán debidamente adoptadas.

De otro lado, y como ya se ha adelantado, no sólo los datos de carácter personal pueden ser objeto de transmisión a un tercero para la prestación de servicios mediante sistemas de computación en la nube. En este sentido, adquieren especial relevancia las transmisiones de información de carácter confidencial y de secretos comerciales, para su ubicación en servidores externos accediendo a los cuales se podrá hacer uso de la misma.

No es objeto de estas líneas poner de relieve la importancia que este tipo de información adquiere para la empresa, ni las nefastas consecuencias que podrían derivarse de un acceso a la misma por terceros no autorizados. Sin embargo, sí procede llamar la atención sobre los riesgos que, en relación con la misma, puede comportar la contratación de servicios de cloud computing que permitan su gestión online. Como se ha dicho, la prestación de estos servicios implica necesariamente la puesta a disposición de un tercero de una información que, por defecto, las empresas acostumbran a almacenar con recelo (un recelo, sin duda, justificado).

Por tanto, y como ya se ha adelantado, la vía contractual –conjugada con el asesoramiento de un experto en la materia- supone la mejor de las garantías para la tranquilidad de las empresas que externalizan el almacenamiento de sus secretos comerciales. A este respecto, resulta especialmente relevante la necesidad de establecer con claridad las medidas de seguridad y el alcance de las mismas, encaminadas a impedir tanto el acceso de terceros no autorizados a la información de la compañía (incluido, en la medida de lo posible- el personal del propio prestador de servicios de Cloud-), como la potencial pérdida de la misma.

8.2.4 Otras cláusulas típicas

Los servicios de Cloud presentan determinadas características para las empresas clientes, en su condición de sujetos pasivos de la actuación empresarial, que pueden resultar muy beneficiosas debido -fundamentalmente- a la reducción de gastos que este modelo, consistente en compartir derechos de propiedad intelectual (software) e infraestructuras informáticas (hardware) con otras empresas, normalmente conlleva.

En primer lugar, la existencia de un "punto único" (one-stop-shop) de tratamiento y almacenamiento facilitado por la empresa prestadora simplifica la estrategia de contratación de los servicios informáticos que ineludiblemente precisan las empresas para su normal desenvolvimiento. Además, el acceso a la prestación de los servicios contratados bajo este esquema puede y debe producirse con enorme agilidad y rapidez, todo ello acompasado con un notable incremento en los niveles de la seguridad física de los entornos tecnológicos utilizados por la empresa cliente.

Asimismo, las empresas disfrutan de una gran flexibilidad en su capacidad de procesamiento de información por el mero hecho de disponer de la posibilidad de escalar masivamente tanto el número como la intensidad en el uso de los servicios informáticos que se prestan.

Definitivamente, estas ventajas conllevan una sustancial mejora en la gestión de los servicios contratados, pero resultaría incoherente no abordar la problemática jurídica que se suscita como consecuencia de su utilización y eludir así la complejidad de las decisiones empresariales que deberán tomarse y de las soluciones que deberán implantarse.

Además de los vistos hasta ahora, muchos otros son los aspectos que también deben tenerse presentes a la hora de elaborar un contrato de prestación empresarial de servicios de Cloud. Así, las cláusulas de propiedad intelectual e industrial son fundamentales en este tipo de acuerdos pues, como resulta evidente, los medios necesarios para prestar los servicios objeto del contrato (programas informáticos, aplicaciones, sistemas de gestión, etcétera) se encuentran protegidos por derechos de este tipo.

En el Cloud, la utilización de tecnología informática permite ofrecer servicios -de utilización de software, de gestión de infraestructuras o de plataformas de sistemas tecnológicos- que, utilizando Internet como medio de comunicación, posibilitan a sus usuarios acceder a determinadas funcionalidades despreocupándose de factores tales como el control de los gastos o la escalabilidad de la capacidad de procesamiento y almacenamiento de toda aquella información con la que se trabaja.

En función de su complejidad, los servicios de Cloud pueden suponer la necesidad de que el beneficiario de los mismos instale en sus propios equipos o materiales algún tipo de programa que permita un fácil acceso a la información y datos que el prestador de servicios está alojando en sus servidores. Por ello, deviene crucial que las partes expresamente reconozcan en el propio contrato que todo uso que con motivo de la materialización de lo dispuesto en el mismo hubieran de hacer de este tipo de obras será, en todo caso, autorizado por el titular de sus derechos o, en su caso, que serán las propias partes (cada una respecto de los elementos que aporte, se entiende) las titulares de los mismos. No es objeto de este capítulo sumergirse en disquisiciones jurídicas respecto del software libre, si bien sí lo es reflejar la importancia de que cada una de las partes se asegure de que la otra acepta mantenerla indemne respecto de cualquier reclamación de un tercero derivada de un uso no autorizado de elementos protegidos por derechos de propiedad intelectual o industrial. En el mismo contexto, el beneficiario de los servicios de Cloud deberá tener presente (y así se tiene por costumbre hacer constar en el contrato)

que el hecho de que el prestador de servicios de Cloud permita a aquél hacer uso de este tipo de elementos, no supone más que eso: un licenciamiento de uso de un software en el que deben contemplarse unas pautas claras de comportamiento tanto en relación con su mantenimiento evolutivo como correctivo. Ello, por supuesto, impide que el beneficiario de los servicios pueda alterar el software, hacer usos distintos, subarrendarlo, etcétera, sin la preceptiva autorización del titular de los derechos o del licenciante si fuera el caso.

Nada desdeñable es tampoco la relevancia de aquellas cláusulas encaminadas a proteger la información, datos y documentación del beneficiario de servicios de Cloud. En muchos casos, la información que las partes intercambiarán puede resultar de una alta sensibilidad (secretos comerciales, asientos financieros) o tratarse de información fundamental y crítica para el negocio. De ahí, que todo contrato empresarial de prestación de servicios de Cloud contenga –en su cláusula correspondiente cuando no en un Anexo específico- los términos más estrictos para lograr la máxima protección para tan valiosa información. Si bien es cierto que las cláusulas con este contenido están considerablemente estandarizadas, su revisión y ajuste por las partes resulta altamente recomendable.

Por último, cabe hacer mención a la importancia de incluir una cláusula relativa a jurisdicción y ley aplicable. A este respecto, las partes podrán acordar la renuncia expresa a cualquier fuero que pudiera corresponderles para la resolución de cuantas controversias pudieran surgir en relación con el contenido del contrato y su correcto cumplimiento. Cláusula típica por excelencia de prácticamente cualquier tipo de contrato, cobra especial relevancia en los contratos de prestación de servicios de Cloud.

Permítasenos aquí hacer alusión a las diversas alternativas disponibles para la resolución de conflictos fuera del ámbito jurisdiccional. Y así, aparte de la negociación entre las mismas partes, deben destacarse los beneficios de la utilización del mecanismo del arbitraje o de la mediación -muy especialmente en el sector tecnológico-, que son por todos conocidos: mayor rapidez, eficacia y, sobre todo, tener la posibilidad de acudir a profesionales con profundos conocimientos técnicos en la materia de que se trate.

Como decimos, un procedimiento judicial en el que concurren elementos internacionales -como suele ser común en el ámbito tecnológico del Cloud- puede extenderse durante años, resultar extremadamente complejo, y, además, comportar costes

elevados. De ahí que, a menudo, aquellos contratos mercantiles más modernos y avanzados prevean la posibilidad de optar por alguno de los citados tres métodos más comunes para la resolución de conflictos sin llegar a juicio: la negociación, la mediación y el arbitraje.

De hecho, en el ámbito internacional el arbitraje se está imponiendo como un método de resolución de conflictos realmente efectivo para las empresas independientemente de su tamaño, pues además de ofrecer una serie de ventajas respecto a la vía judicial ordinaria, puede evitar a las partes el sometimiento a jurisdicciones extranjeras que puedan ser totalmente desconocidas. De ahí que la fase de negociación de los contratos se presente como el momento ideal para fijar el compromiso de sometimiento a un sistema arbitral ante una posible controversia futura. Y es que, en ese momento, las partes están imbuidas por una firme voluntad de acuerdo y un sentido de mutua ganancia.

9. LA IMPORTANCIA DE LOS ANEXOS

En ocasiones se critica que el modelo Cloud limita sustancialmente la libertad de gestión por parte de las empresas clientes y las convierte en empresas excesivamente dependientes de sus proveedores de servicios. El modelo Cloud Computing implica la presencia de "terceras empresas proveedoras de servicios" que intervienen tanto en la gestión de la información que se utiliza o se genera en los procesos productivos de las empresas como a la hora de permitir el acceso a las redes de telecomunicación de Internet.

Si los datos personales de los que son responsables las empresas se encuentran en manos de terceros (como encargados de su tratamiento), o si llega a producirse una indisponibilidad de acceso a Internet podrían potencialmente generarse condiciones de alta vulnerabilidad para la empresa cliente, circunstancias estas que deben ser apropiadamente valoradas por los directivos de las compañías a la hora de implantar en una determinada organización soluciones basadas en el modelo Cloud.

Por ello, el contrato marco, como tal, es indudablemente importante para la seguridad de la prestación de los servicios que hasta aquí se han venido describiendo; el apartado anterior resulta esclarecedor de tal afirmación. Sin embargo, la complejidad de los servicios pactados, en innumerables ocasiones impide, de un lado, una configuración ordenada de todos los aspectos a tener en cuenta y, de otro, la gestión y el asesoramiento en la elaboración del contrato por un profesional desconocedor de las intrincadas bases técnicas que soportan los servicios de Cloud. La necesidad de claridad a la que quedan sometidos los contratos en general, es mayor aún en aquellos que recojan una prestación de servicios técnicamente complejos. Es el caso del Cloud.

Dos objetivos fundamentales se persiguen con la búsqueda de claridad: evitar erróneas interpretaciones del contenido por alguna de las partes (o interpretaciones paralelas, contrarias o no coincidentes) y facilitar la interpretación del sentido del contrato por un tercero ajeno a la relación que tuviera que decidir respecto del significado de cualquiera de las cláusulas, respecto de la intención de las partes, respecto de los límites u obligaciones que establecen o respecto del correcto cumplimiento de lo estipulado (piénsese en un tribunal, árbitro o mediador que hubiera de enfrentarse a un contrato de Cloud que no presentara la claridad y el detalle necesarios). Fruto de esta búsqueda de claridad y de acuerdo en la terminología, surgen los anexos que, por ejemplo, contienen listados de definiciones sobre los principales términos –generalmente de carácter técnico- sobre los que es fundamental que las partes estén de acuerdo.

Sin embargo, probablemente el anexo más relevante a elaborar en la creación de un contrato empresarial de servicios de Cloud sea el que contiene el Acuerdo de Nivel de Servicio. Dadas las características de los servicios de Cloud, en particular en lo tocante a la complejidad técnica de la infraestructura sobre la que se soportan tales servicios, deviene fundamental el establecimiento de una serie de condiciones que regulen el mantenimiento de la misma en condiciones óptimas.

El traslado a la "nube" de funcionalidades e información tradicionalmente alojadas en servidores de la propia compañía beneficiaria de los servicios de Cloud debe permitir a ésta tener acceso a las mismas en cualquier momento y en cualesquiera circunstancias, incluso, desde cualquier ubicación (siendo, como ya se ha dicho con anterioridad,

fundamental disponer de conectividad para ello). Es frecuente que se contemple contractualmente que la propia empresa prestadora de servicios de Cloud se encargará del mantenimiento y seguridad de los sistemas que alojen la información.

Sin embargo, ese mero compromiso queda lejos de evitar potenciales conflictos respecto de las condiciones en que se llevará a cabo el mantenimiento del servicio y la solución de cuantos problemas de accesibilidad imputables al prestador de servicios de Cloud pudieran surgir o de aquellos relativos a la calidad de la prestación. Lejos queda también el simple pacto de establecer como merece cuáles son los niveles correctos exigibles a este respecto.

Por ello, la contratación de servicios de Cloud, el contrato mismo, deberá ir acompañado del denominado Acuerdo de Nivel de Servicio o ANS (también habitualmente denominado por el término inglés Service Level Agreement o por sus siglas SLA). Tales Acuerdos comenzaron a emplearse en la década de 1980 por los operadores de telecomunicaciones, mediante los cuales acordaban con sus clientes empresariales unas condiciones mínimas de prestación del servicio, pues las comunicaciones electrónicas devenían ya en aquellos días fundamentales para el correcto desarrollo de la actividad empresarial. De ahí la necesidad de articular un sistema de responsabilidad para el operador respecto de la calidad del servicio a prestar a las empresas.

De las innumerables definiciones que pueden encontrarse del concepto de Acuerdo de Nivel de Servicio, especialmente significativa resulta la ofrecida por el Department of Commerce del Gobierno estadounidense en un documento sobre seguridad y privacidad en el ámbito del Cloud computing:

«Un ANS representa el acuerdo entre el beneficiario del Cloud y el prestador de servicios de Cloud respecto del nivel esperado del servicio a prestar y, en el supuesto de que el prestador no ofreciera el servicio a los niveles especificados, la compensación disponible para el beneficiario de los servicios de Cloud. Un ANS, sin embargo, por lo general constituye solo una parte de los términos de servicio estipulados en el conjunto del contrato o acuerdo de servicios. Los términos de servicio cubren otros detalles de importancia, tales como las licencias de servicios, los criterios de uso aceptable, la

suspensión y terminación del servicio, límites a la responsabilidad, política de privacidad y modificaciones de los términos de servicio».

En definitiva, los Acuerdos de Nivel de Servicio, conforman una parte fundamental de la contratación empresarial de servicios de Cloud, encaminada a asegurar la correcta prestación de los servicios en cuestión, de manera que la misma satisfaga las necesidades de la compañía contratante. Pese a ser esenciales, sin embargo, son precisamente eso: una parte del contrato; y ello, porque el resto del mismo contendrá, entre otros, todos los aspectos analizados con anterioridad en este capítulo, sin los cuales la configuración de los servicios a prestar y del acuerdo mismo carecería de la integridad necesaria.

De otro lado, la definición ofrecida apunta ya lo que también será objeto de comentario más adelante en el presente apartado y que habitualmente se encuentra contenido en el propio ANS: el régimen de responsabilidad por incumplimiento de lo contenido en el Acuerdo de Nivel de Servicio, distinto del régimen general establecido para el supuesto de incumplimiento de cualesquiera otras obligaciones contenidas en el contrato.

Generalmente conformados como anexos al contrato, los Acuerdos de Nivel de Servicio establecen una serie de parámetros objetivos acordados entre las partes mediante los que se concretan los grados de cumplimiento del servicio y/o los modos de proceder ante problemas de carácter técnico que pudieran surgir, tiempos de reacción ante tales problemas, tiempos de resolución de los mismos, disponibilidad de agentes encargados del mantenimiento, disponibilidad del servicio en sí mismo, niveles máximos o mínimos de disponibilidad de determinados valores (a modo de ejemplo: de suministro eléctrico, cantidad máxima de paquetes de datos cuya pérdida se entenderá como justificada, niveles de gravedad de incidencias, etcétera).

Dado el carácter eminentemente objetivo de los parámetros reflejados en el Acuerdo de Nivel de Servicio, el detalle con que las partes deberán acordar cada extremo de los reflejados en el mismo deberá ser suficiente para poder determinar en qué casos se está produciendo un incumplimiento de los mismos. Tal es así, que los Acuerdos de Nivel de Servicio generalmente descienden a medidas cuantificadas incluso en minutos (para concretar, por ejemplo, los tiempos de respuesta o de resolución de una incidencia), pues

la falta de concreción vaciaría de contenido el propio Acuerdo, siendo imposible determinar de modo objetivo el cumplimiento de los niveles de calidad pactados.

De lo anterior, por tanto, puede extraerse una conclusión sólo parcialmente obvia: la relevancia de que ambas partes aseguren el empleo en el Acuerdo de Nivel de Servicio de un lenguaje lo suficientemente claro como para evitar interpretaciones dispares tanto respecto de los indicadores o parámetros detallados como de las unidades de medida empleadas. Y ello, únicamente podrá lograrse si las partes afrontan su elaboración desde actitudes basadas en el principio de buena fe que se presupone a la negociación de un contrato que deberá ser beneficioso para ambas, siendo deseable una actitud especialmente colaborativa que facilite el entendimiento e impida el surgimiento de interpretaciones contrarias del contenido del Acuerdo de Nivel de Servicio.

Es igualmente común que el propio Acuerdo de Nivel de Servicio contemple la posibilidad de revisión (dentro de unos plazos conferidos por las partes al efecto) tanto de los parámetros contenidos en el mismo como de la cuantificación de los mismos. Y ello porque en multitud de ocasiones las partes no alcanzan la precisión deseada respecto de la calidad y grado de mantenimiento de los servicios mediante una mera teorización a priori de los mismos. No es infrecuente la necesidad de ajustar el contenido de los Acuerdos de Nivel de Servicio una vez puesta en marcha la prestación de los servicios de Cloud y comprobada la eficiencia de las medidas adoptadas para el aseguramiento de la calidad que el cliente necesita para el correcto desarrollo de su actividad empresarial.

Por otra parte, no se puede por menos que hacer mención del régimen de responsabilidad asociado a los incumplimientos del Acuerdo de Nivel de Servicio. Tal y como ya ha quedado dicho, tal régimen de responsabilidad difiere del configurado para supuestos de incumplimiento contractual de carácter general, en primer lugar, porque al que aquí nos referimos se limita exclusivamente a la inobservancia de lo dispuesto en el Acuerdo de Nivel de Servicio frente al incumplimiento contractual de carácter general al que se vincula el régimen de responsabilidad stricto sensu.

En algunas ocasiones, el propio Acuerdo de Nivel de Servicio contempla las penalizaciones a aplicar al prestador de servicios de Cloud por incumplimiento de lo establecido en el mismo. Sin embargo, no es poco habitual encontrar el desarrollo de las

mismas conformando un anexo separado del anterior –si bien, formando aún parte del mismo contrato de prestación de servicios de Cloud-.

Los términos que sirven de base para la configuración de las penalizaciones por incumplimiento de las condiciones establecidas en el Acuerdo de Nivel de Servicio pueden adoptar diversas estructuras, siendo en todo caso de carácter económico. Si bien las fórmulas empleadas para la cuantificación de la sanción pecuniaria a abonar en supuesto de incumplimiento pueden alcanzar gran complejidad, por lo general incluyen una serie de parámetros comunes, a saber: la diferencia en la prestación respecto del umbral marcado como objetivo en el Acuerdo de Nivel de Servicio y un importe tomado como referencia (que puede ser la cuantificación del beneficio que se hubiera obtenido si el resultado de la actuación hubiera sido satisfactorio o bien una cantidad a tanto alzado). Es decir, cuanto mayor fuera la desviación respecto de los parámetros acordados como correctos, mayor resultaría el importe a abonar como penalización.

En definitiva, la relevancia que en las últimas décadas han adquirido los Acuerdos de Nivel de Servicio y, consecuentemente, el detalle de las penalizaciones por incumplimiento del mismo, dan una clara idea de la importancia no solo de que el servicio de Cloud sea prestado, sino que la prestación del mismo tenga lugar en condiciones óptimas. De ahí, que con frecuencia las partes acuerden Acuerdos de Nivel de Servicio de complejísimo contenido técnico, siendo necesaria la participación en su configuración de expertos en la materia.

10. ALGUNOS ASPECTOS LABORALES

En la medida en que la gestión de los sistemas utilizados en el modelo de computación en la nube es desempeñada por un tercero, el cumplimiento del deber de vigilancia de la actividad de los empleados por parte de la empresa cliente se ve de algún modo limitada. Sin embargo, tanto la empresa proveedora de servicios en la nube, como la empresa cliente mantienen la obligación de establecer los mecanismos adecuados con el fin de que se produzca el adecuado uso de los servicios tanto por los propios empleados como por parte de los empleados de la empresa cliente.

Es importante destacar que el establecimiento de estos mecanismos provoca ineludiblemente la aparición de un riesgo de intromisión en los derechos a la intimidad del trabajador, mientras que –en paralelo- la misma posibilidad de acceder desde cualquier punto de conexión a la información depositada en los servidores de computación en la nube, puede conducir a un uso fraudulento de la identidad de los usuarios finales (también, potencialmente, trabajadores de la empresa cliente), si –entre otras medidas - no se implanta un sistema a través del cual se procura una rigurosa gestión de los controles de acceso por parte de esos trabajadores. Un sistema excesivamente laxo de gestión de los nombres de usuario y de sus correspondientes contraseñas puede dar lugar a la violación de las obligaciones de confidencialidad asumidas por las empresas en relación con terceros y la consiguiente extracción no deseada de información de los sistemas por parte de terceros no autorizados.

La implantación de los denominados "protocolos de utilización de herramientas informáticas y tecnológicas en el puesto de trabajo" se presenta en el modelo de computación en la nube como una obligación más que inexcusable al objeto de delimitar el uso que los trabajadores pueden realizar de las aplicaciones ubicadas en la nube.

En paralelo, este protocolo debe tener su reflejo en la inclusión en el contrato laboral de ciertas cláusulas, de tal forma que su incumplimiento por parte del trabajador –como, por ejemplo, la obligación de secreto de la información a la que se tiene acceso- pueda resultar en la adopción de las correspondientes acciones disciplinarias que en materia laboral sean de aplicación. En todo caso, las medidas impuestas por parte de las empresas (tanto proveedoras de servicios en la nube como de empresas clientes de estos servicios) deben guardar una adecuada proporcionalidad con los objetivos que se persiguen, no implicar la utilización de medios intrusivos y deben estar debidamente justificadas en relación con los propósitos perseguidos en el marco de la contratación efectuada.

En el protocolo se establecerá el modo en el que se generarán las evidencias electrónicas así como su procedimiento de obtención, conservación y aportación. Asimismo, en dicho protocolo deberá especificarse la persona responsable que en el seno de la propia empresa realizará el seguimiento y el control de la actividad en la nube por

parte de los trabajadores -tanto en el ámbito profesional como en privado, si fuese el caso- y cuyo alcance, lógicamente, dependerá de las características propias de las aplicaciones, infraestructuras o plataformas que sean objeto de contratación por parte de las empresas.

11. ALGUNAS CONSIDERACIONES PENALES

El 23 de diciembre de 2010, entró en vigor la reforma del Código Penal (Ley Orgánica 5/2010 de 22 de junio) por la que se incorpora por vez primera a nuestro Ordenamiento Jurídico, la responsabilidad penal de las personas jurídicas.

Los ilícitos cuya comisión es más factible por parte de una empresa proveedora de servicios de Cloud, son aquellos que recaen sobre los activos de información de los que es responsable el cliente (revelación de secretos, violación del secreto de las comunicaciones, delitos contra la propiedad intelectual e industrial, etc.) y entre ellos, los que recaen sobre los datos de carácter personal, en los que además de responder penalmente, habrá cometido una infracción administrativa (además de su respectiva responsabilidad civil, frente al responsable del fichero y frente al afectado, respectivamente).

La propia LSSI antes mencionada expresamente establece que, sin perjuicio de lo dispuesto en la misma, los prestadores de servicios de la Sociedad de la Información (entre los que, como se ha dicho, se encuentran las empresas de Cloud) están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico.

Es responsable penal la persona jurídica como tal respecto de los delitos cometidos en su nombre o por su cuenta y en su provecho por las personas que tienen poder de representación en las mismas (los administradores de hecho o de derecho y representantes legales) así como por sus empleados cuando la empresa no haya realizado el debido control sobre éstos (art. 31 bis CP). La responsabilidad penal de la persona jurídica se podrá declarar con independencia de que se pueda o no individualizar la responsabilidad de la persona física que tiene la capacidad de representar a la empresa. En

todo caso, la responsabilidad de las personas morales no viene a sustituir la de sus administradores que pueden llegar a sufrir penas de prisión

Por ello, con la reciente reforma del Código Penal español, se ha incrementado el riesgo de que un directivo sea imputado e incluso condenado por la mala conducta de un trabajador de la empresa o, incluso, por una decisión operativa o estratégica.

Esta reforma viene a recordar de manera más perentoria a las empresas a las que pueda resultar de aplicación del Código Penal español, la necesidad de implantar un sistema de supervisión y control de cumplimiento normativo como mecanismo indispensable y eficaz de prevención y mitigación de su responsabilidad penal.

En paralelo, el legislador también ha querido premiar a las sociedades más diligentes por lo que su responsabilidad penal se verá atenuada en caso de que se produzca:

a) Confesión de la infracción ante las autoridades

b) Colaboración en la investigación del hecho delictivo

c) Reparación del daño causado por el delito

d) Establecimiento de medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica

Más concretamente, en el ámbito del Cloud, podemos mencionar que si la empresa proveedora de servicios no despliega unas políticas de control interno que resulten suficientes para crear un clima favorable para que sus directivos y empleados comentan delitos, puede ser penalmente responsable, al igual que si no ejerce la vigilancia debida sobre los mismos (culpa invigilando).

Por ello, resulta muy aconsejable que las empresas dispongan de sistemas de prevención, medidas de vigilancia y control que permitan evitar o detectar la posible comisión de ilícitos penales. De este modo, la compañía estará en mejor posición para acreditar la realización del debido control sobre sus empleados y por lo tanto atenuar la responsabilidad derivada de la nueva regulación del Código Penal.

Estas actuaciones se deberán implementar en las empresas a través de un plan preventivo integral dirigido a identificar, prevenir y mitigar riesgos penales de origen corporativo.

Para ello, se deberá analizar y regularizar la documentación jurídico-financiera de la empresa (tanto en soportes físicos como digitales) y los procedimientos relacionados con la producción, operaciones y administración (calidad, ISO, procesos, productos, relaciones laborales, etc.).

Y en el área más puramente tecnológica, deberán ponerse en práctica acciones conducentes a la elaboración de:

I. Códigos éticos de buen gobierno corporativo.

II. Programas de cumplimiento corporativo que garanticen el cumplimiento de la ley.

III. Preparación de un programa con contenido "informático forense" que permita la trazabilidad y generación de la prueba en los sistemas informáticos.

IV. Normas de organización interna en materia informática y tecnológica.

V. "E-discovery": programas de revisión de la documentación depositada en formato digital.

VI. Comités de vigilancia y supervisión tanto física cómo lógica del que deben formar parte consejeros independientes.

Los prestadores de servicios de Cloud, por tanto, pueden llevar a cabo conductas expresamente tipificadas como faltas o delitos en el Código Penal, de las que pueden a su vez resultar afectados los destinatarios de tales servicios. En este sentido, y sin perjuicio de cualesquiera otros que pudieran resultar de aplicación según el supuesto concreto, procede aquí hacer mención a un conjunto de artículos del Código Penal Español.

Así, en los delitos relativos a la propiedad industrial, la intervención penal relativa a la propiedad industrial se centra en dos sectores de la actividad mercantil, el que abarca las creaciones industriales, por un lado, y el relativo a los signos distintivos, por otro. En concreto, la intervención punitiva va encauzada a la protección de: las patentes, modelos de utilidad y la protección de las marcas (Art. 273 y 274 CP).

En el delito de espionaje industrial (Art. 278 CP), la conducta típica consiste en el descubrimiento de un secreto de empresa, apoderándose de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos y, además, constituye un tipo agravado el apoderamiento seguido de la difusión. Lo dispuesto respecto a este delito es independiente de las penas que puedan corresponder por el apoderamiento o la destrucción de los soportes informáticos (hurto, robo, etc.).

La violación de los deberes de reserva (Art. 279 CP) consiste en el descubrimiento de secretos por parte de quien ha tenido acceso a los mismos de forma legítima, pero viola las reglas que exigen el mantenimiento del mismo por tener legal o contractualmente obligación de guardar reserva con respecto a él. La acción típica consiste en difundir, revelar o ceder el secreto, diferenciándose del caso anterior tan sólo en la forma de acceder al mismo. En este sentido, el art. 279.2 CP contiene un tipo privilegiado que reduce la pena al sujeto que viola los deberes, no de reserva frente a terceros, sino de aprovechamiento personal del secreto frente a quien se lo ha facilitado legalmente.

Así, a modo de ejemplo, aquellos proveedores de servicios de Cloud que se apoderen, utilicen o modifiquen, en perjuicio de un tercero, tanto datos de carácter personal como datos relacionados con las comunicaciones que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos podrán estar incurriendo en un delito de descubrimiento o revelación de secretos tipificado por el código penal. A su vez, en caso de tratarse de datos de carácter personal, la pena se agravará si el infractor, en su calidad de encargado o responsable de los ficheros, difundiera, revelara o cediera a terceros los datos en cuestión. Con independencia del mayor detalle con que siempre podría abordarse esta cuestión, resulta -a los efectos que aquí interesan- significativo que el legislador penal es bien consciente de la posición relevante que ostenta cualquiera que pudiera tener, de manera general, acceso a información de terceros .

En el área de lo que se define con mayor precisión como el delito informático, el art. 264 CP hace extensible la responsabilidad por este delito a las personas jurídicas, incurriendo con ello en penas de multa u otras a juicio de los jueces y tribunales. La conducta típica se produce cuando el objetivo de la actividad realizada es dañar, alterar, suprimir o hacer inaccesible datos o programas electrónicos ajenos. En lo que se refiere al continente del objeto destruido, alterado, inutilizado o dañado, los datos, programas o documentos electrónicos deben hallarse en redes, soportes o sistemas informáticos.

De la literalidad de la norma podemos inducir que el medio utilizado para cometer la acción puede ser 'cualquier medio'. Con ello se engloba cualquier posibilidad, y por tanto, la norma jurídica iguala, por tanto, un acto de destrucción física a un acto de manejo de un ordenador.

Sin que deba atenderse en absoluto que una empresa de Cloud tenga por objeto la realización de las conductas a las que nos referiremos a continuación, a través de los medios de los que dispone un prestador de servicios de Cloud Computing pueden realizarse actividades fraudulentas consistentes -por ejemplo- en la creación de ficheros informáticos “paralelos” produciendo un error en el usuario que tendrá la idea de estar actuando en un entorno distinto del real.

Este tipo de actividades son con frecuencia ejecutadas con el fin de llevar a cabo transacciones fraudulentas, definidas en el Código Penal (art. 248 CP) como aquellas que, utilizando engaño bastante mediante manipulación informática o artificio semejante para la producción de error en un tercero, induzca a éste a realizar actos de disposición o transferencias no consentidas de activos patrimoniales en perjuicio propio o ajeno

Obviamente, a través del modelo de Cloud Computing podrían llegar a proliferar estafadores cuya actividad delictiva consista en la creación de páginas web de Internet falsas cuya finalidad consistiría en apropiarse indebidamente de información volcada por los usuarios, así como en realizar acciones tendentes a modificar o a sustituir el archivo del servidor de nombre de dominio, dando lugar a un cambio de la dirección IP legítima de una entidad e induciendo a que cuando el usuario escriba el nombre de dominio sobre la barra de direcciones, el navegador lo redirija a una dirección IP falsa. Una vez que se ha redireccionado al usuario a la página web de Internet fraudulenta, el estafador podría

obtener aquellos datos personales pertenecientes a la víctima así como la información confidencial necesaria para realizar transacciones fraudulentas. Como decimos, la actividad que aquí se describe encontraría un encuadre en el tipo penal del fraude online, recogido en el artículo 248 del Código Penal.

En relación con las posibles colisiones con los derechos de propiedad intelectual, la nube podría llegar a ser un entorno inseguro para poner a disposición del público determinados contenidos sujetos a derechos de propiedad intelectual de consumo típicamente lineal como pueden ser los libros electrónicos, las películas, música, etc. Sin embargo, sí puede ser un entorno seguro y atractivo para aquellos contenidos sujetos a derechos de propiedad intelectual de consumo interactivo como los videojuegos o el software que sólo se pueden ejecutar en la nube, sin que se deba acceder al archivo que los contiene en un determinado servidor y sin que se deban llevarse a cabo copias o su instalación en el terminal propio del usuario.

El artículo 270 del código Penal es un precepto que contiene importantes elementos normativos que deben ser interpretados acudiendo a la legislación reguladora mercantil y civil. En ese artículo se describen las acciones que resultan sancionables y establece la exigencia de un dolo específico, esto es, obrar con ánimo de lucro y en perjuicio de tercero. Esta frase implica que el delito se consuma con la realización de la conducta típica sin que sea necesario que se llegue a producir "de hecho" un perjuicio en el titular de los derechos o que se logre el lucro perseguido. Sin embargo, no habrá delito cuando falte el ánimo de lucro, como es el caso, de quien realiza una copia privada sin autorización del titular. El elemento subjetivo exigido, esto es, el ánimo de lucro, no puede tener una interpretación amplia o extensiva sino que ha de ser entendido sentido estricto de lucro comercial. Por ello, las conductas para la comunicación u obtención de obras protegidas en Internet o utilizando nuevas tecnologías de la información -como colocar en la red o bajar de Internet- no son oponibles si no concurre ánimo de lucro comercial.

Este artículo del código Penal recoge en su texto cuatro conductas básicas: la reproducción, el plagio, la distribución y la comunicación pública de las obras. Y en relación con ellas, son tres las circunstancias necesarias que los hechos encuentren encajen en el tipo delictivo: la primera, una acción de reproducción, plagio, distribución o comunicación pública de una obra literaria artística o científica o de transformación,

interpretación o ejecución de las mismas en cualquier tipo de soporte o su comunicación por cualquier medio; la segunda, la carencia de autorización para cualquier clase de esas actividades por parte de los titulares de los correspondientes derechos de propiedad intelectual; y la tercera, la realización intencionada de esas conductas con la concurrencia de dolo específico, esto es, ánimo de lucro.

En todo caso, en el modelo cloud las empresas clientes podrían desear acceder y usar los servicios prestados de acuerdos con sus propias necesidades, beneficiándose del acceso a los servicios, contenidos y software que proporciona la empresa proveedora. Sin embargo, en determinados casos las empresas clientes también perseguirán que los derechos de propiedad intelectual que ellas generen sobre sus propios contenidos o el nuevo software (original o derivado) creado o almacenado en la nube queden debidamente protegidos.

Una de las soluciones que se imponen pasaría por introducir en el contrato que rige la prestación de servicios en la nube y en la política de uso o de acceso a la nube las cláusulas tendentes a establecer el equilibrio necesario entre la responsabilidad debida por las empresas clientes al ejecutar y usar los contenidos, servicios y software ajenos desde la nube y las medidas de seguridad tendentes a proteger los derechos de propiedad intelectual que deberán ser garantizados por la empresa prestadora de servicios.

En esta misma línea conviene destacar que la utilización de las aplicaciones alojadas en la nube puede dar lugar a la generación de creaciones intelectuales merecedoras de protección en materia de derechos de propiedad intelectual, por lo que resulta muy aconsejable incluir en el contrato cláusulas dirigidas a establecer el régimen de titularidad o de co-titularidad de los derechos de propiedad intelectual relativos a las creaciones intelectuales que pudieran generarse bajo el modelo de negocio de la nube.

Existe así mismo la posibilidad de que las empresas clientes utilicen los servidores en la nube para almacenar contenidos o software ajenos como forma –a su vez- de prestar servicios a terceros, de forma que queden alojadas copias de contenidos y de software en servidores de almacenamiento remoto desde los cuales que posteriormente puedan realizarse reproducciones. Cuando este tipo de servicios se prestan en la manera descrita, las empresas clientes ponen a las empresas proveedoras de estos servicios en la nube en riesgo de una responsabilidad jurídica en función de las potenciales infracciones de

derechos de la propiedad intelectual que pudieran producirse. Si este fuese el caso, resulta necesario incluir en el contrato de servicios en cloud la asunción expresa e inequívoca por parte de las empresas clientes de toda responsabilidad jurídica que pudiera surgir con motivo de estos actos potencialmente ilícitos, mediante la incorporación en el contrato y en la política de uso de los servicios en la nube de aquellas previsiones a través de las cuales la empresa prestadora de servicios pueda reservarse a su favor la facultad tanto de hacer un seguimiento como de eliminar aquellos contenidos y software ajenos que los usuarios terceros puedan incluir en los servidores de la nube, estableciéndose para ellos determinados criterios como que puedan afectar a derechos de terceros, intereses u orden públicos, etc.

La deslocalización internacional –característica propia de la prestación de servicios en la nube- puede dar lugar en ocasiones a la utilización del contenido ajeno, software ajeno o de servicios que se prestan desde jurisdicciones donde está prohibido su uso o el mismo no se encuentra autorizado. Por ello, se hace necesario contemplar en el contrato regulador de estos servicios las restricciones que deban regir respecto del uso de los servicios en la nube en relación con aquellos territorios desde donde no resulta lícito su utilización, así como establecer los más adecuados mecanismos de control tecnológico de forma que ese contenido o software ajeno no pueda ser ejecutado en tales territorios. Otra solución jurídica viable consistiría en renegociar y ampliar las licencias firmadas entre los terceros proveedores de software, contenidos o servicios y la empresa proveedora de servicios en la nube para que las empresas clientes puedan utilizar lícitamente tales derechos desde cualquier jurisdicción.

En definitiva, puede entenderse que el entorno de Internet -en general- y el de los servicios de Cloud Computing -en particular- podrían servir de medio para la realización de conductas delictivas, lo que, sin embargo, no debe constituir una señal de alarma mayor que la que pudiera entenderse en entornos no digitales.

12. LEY APLICABLE Y TRIBUNAL COMPETENTE

Tampoco son aspectos menores la determinación de la legislación y jurisdicción aplicables a cualquier contrato. Es más, en ocasiones puede resultar un aspecto clave debido a que no es improbable la aparición de un conflicto entre jurisdicciones por encontrarse la información ubicada físicamente en un territorio distinto de aquel en que se encuentren los contratantes y, como consecuencia, resulte aplicable un régimen jurídico distinto, y competentes unas autoridades distintas, un sistema judicial distinto a los que a priori podamos pensar como "lógicos u obvios".

El lugar físico de ubicación de los servidores en un Estado concreto viene a determinar, como norma general, tanto la legislación como la jurisdicción aplicables. Sin embargo, aunque pueda resultar complicado determinar dónde se ubican los servidores en los que se aloja la información y resulta complejo determinar qué norma puede llegar a aplicarse en cada momento, este hecho no debe servir para excusar el incumplimiento por parte de las empresas que prestan servicios de cloud computing de los principios jurídicos de la protección de datos y la privacidad que protegen a los ciudadanos.

Un potencial problema que no debe pasar inadvertido consiste en que las autoridades de un determinado país pueden llegar a tener competencia para “confiscar” tal información. Una posible solución a este potencial conflicto puede pasar por que el proveedor de servicios de cloud computing se obligue contractualmente a no transferir en ningún caso información a otros países sin el previo consentimiento expreso del cliente.

13. CONCLUSIÓN

En definitiva, las bondades de los servicios de cloud computing resultan obvias a la luz del vertiginoso crecimiento que se observa en el sector. Sin embargo, no es menos cierto que los riesgos que puede comportar su contratación pueden afectar a aspectos altamente relevantes para la seguridad del negocio de una compañía, aunque una gestión

adecuada de tales riesgos pueda resultar en un ahorro de costes y una mejora de la eficiencia productiva de la empresa.

La existencia de los potenciales riesgos jurídicos arriba descritos, sin embargo, no supone que deba necesariamente desaconsejarse la contratación de servicios de cloud computing. Por el contrario, una prestación responsable de servicios de computación en la nube que permita a las empresas la gestión remota de su información dará lugar a un ahorro de costes –principalmente derivados del almacenamiento y procesamiento de información-, incluso teniendo en consideración la posible necesidad de una mayor inversión en condiciones de conectividad a Internet o de alguna estructura específica de hardware residente.