Ponencia presentada al

XIX Congreso Iberoamericano de Derecho e Informática, Medellín, 26-28 de agosto de 2015, Universidad Pontificia Bolivariana

PROTECCIÓN DE DATOS Y SERVICIOS PÚBLICOS Y PRIVADOS DE CLOUD COMPUTING EN ESPAÑA Y EUROPA

Lorenzo Cotino Hueso (www.cotino.es), Profesor titular, Catedrático de Derecho Constitucional de la Universidad de Valencia, coordinador de la Red de especialistas en Derecho de las Nuevas Tecnologías de la Información y Comunicación (TICs) www.derechotics.com [1]

Dirección postal: Facultad de Derecho, Universitat de Valencia. Edificio Departamental Central Avda. de los Naranjos s/n 46071-Valencia.

Teléfono (+34) 96 3828120

e-mail: Lorenzo.Cotino@uv.es

Resumen:

El estudio describe en qué consisten los servicios de la nube y sus perspectivas, para señalar los riesgos y problemas más importantes que suscita, en particular respecto de la seguridad y la privacidad. A este respecto se señalan algunas deficiencias de la vieja y superada regulación nacional y europea de protección de datos aplicable a la nube, corregidas en alguna medida por la acción de instituciones de protección de datos en los últimos años. Se observa también la proyección del esperado reglamento europeo de protección de datos, ya por la figura del delegado de protección de datos y, sobre todo, por las exigencias de privacidad por diseño y por defecto que se

[1] www.cotino.es (ahí puede accederse al texto completo de muchas publicaciones). El presente estudio se realiza, de una parte, en el marco Convenio entre la Universitat de València y la empresa de servicios en la nube Occentus Network sl, en el marco de la ayuda para la realización de una estancia de personal investigador en empresas de la Comunitat Valenciana (AEST/2015/023). Asímismo, en el marco del Proyecto "Régimen jurídico constitucional del Gobierno 2.0-Open government. Participación y transparencia electrónicas y uso de las redes sociales por los poderes públicos" (DER2012-37844), del Ministerio de Economía español y de la investigación con la Universidad Unisabaneta "Gobierno abierto: participación, transparencia, datos abiertos, colaboración y gobierno en línea. Problemas y barreras jurídicas al desarrollo".

concretarán en futuras normas técnicas del sector que habrá de aprobar la Comisión Europea. Se expone la tendencia a reforzar las obligaciones del prestador de servicios de nube (normalmente una gran corporación), que es "encargado", para que el cliente de la nube, que es el "responsable", pueda cumplir sus tiene obligaciones de diligencia y responsabilidad. Igualmente se detallan exigencias respecto del conjunto contractual y la subcontratación de servicios y las diversas vías de flexibilización de la necesidad de autorización de las transferencias internacionales de datos con terceros países que el uso de la nube frecuentemente supone (cláusulas contractuales tipo y *Binding Corporate Rules*). Para concluir se hace una breve aproximación a algunas exigencias jurídicas de los servicios de la nube cuando son prestados a las administraciones públicas en España.

1. La cara y la cruz de los servicios de la nube

Que la nube es un futuro ineludible que es ya presente, no hay duda. Que su uso genera toda una serie de retos y cuestiones jurídicas, tampoco. La atención científica y académica de la nube se ha centrado, como es normal, en los aspectos tecnológicos. Sin embargo, pese a ser esencial el enfoque jurídico para el desarrollo del *cloud*, no es mucha la literatura jurídica española sobre la materia, aunque con estudios muy destacables[2], como en México[3]. Es algo mayor la atención en el ámbito europeo y anglosajón[4], o de EEUU[5]. Pese a que son diversas las cuestiones jurídicas que suscita nube, por razones de espacio,

[2] En español, sin perjuicio de las obras que se citan más adelante, una pionera atención los trabajos de Leenes y Miralles en *IDP. Revista de Internet, Derecho y Política*. N.º 11. UOC. Especialmente destaca la monografía MARTÍNEZ i MARTÍNEZ, Ricard (2013). De especial valor son los documentos institucionales de la AEPD (2013) y del GRUPO DEL ARTÍCULO 29 (2012)

[3] En México, una descripción completa del tema en TÉLLEZ VALDÉS (2014).

[4] Hay estudios iniciales, como VAN GYSEGHEM (2010) En cualquier caso, en Europa destacan sin duda alguna los distintos estudios jurídicos realizados en los últimos años y publicados desde el Queen Mary School of Law Legal Studies en razón del cloudlegalproject.org con apoyo de Microsoft. Y desde 2014 se insittuye el Microsoft Cloud Computing Centre (www.mccrc.eu/) del Queen Mary con la U. de Cambridge. Se puede acceder a casi todas las publicaciones jurídicas tanto en SSRN como en cloudlegalproject.org, aunque no a la monografía MILLARD de (2013).

[5] Sobre el régimen jurídico de la nube en Estados Unidos SOLOVE (2014). Y sobre disparidades y posibles choques entre normativa americana y europea de protección de datos para la nube, SCHWARTZ, (2013).

el presente estudio focaliza el análisis en lo más vinculado a seguridad y protección de datos y algunas cuestiones vinculadas al uso de servicios de cloud por las Administraciones. Ello sin perjuicio las crecientes facultades -y dificultades- de investigación de la nube y los deberes de colaboración de las empresas[6].

1.1 La cara: aproximación a los servicios de la nube, una de las mayores revoluciones tecnológicas de los últimos tiempos y a su importancia económica y social

El desarrollo de los sistemas informáticos ha evolucionado, se puede decir que de manera natural[7], hacia la nube, el *cloud computing*. En un lustro, buena parte de la información mundial estará en la nube, ya se trate de información pública o de sujetos privados, ya se trate de información privada o reservada o información de libre acceso. Pese a algunos escépticos sobre su importancia[8] Estamos ante una de las mayores revoluciones tecnológicas de los últimos tiempos. Y, como cualquier proceso evolutivo, el avance de la computación en nube como paradigma tecnológico mundial representa un desafío en todos los órdenes.

---

[6] Sobre el tema, mi ponencia "Derechos fundamentales e investigación criminal de la información que está en la *nube*", en el Congreso Internacional "Seguridad en libertad", Universidad de Konstanz, 15 – 21 de junio de 2015. Al respecto, hay que tener especialmente en cuenta el Proyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal aprobado el 13 de marzo de 2015, que regula el "registro de dispositivos de almacenamiento masivo de información". Especialmente hay que tener en cuenta el artículo 588 septies a) y el esencial deber de colaboración de los prestadores regulado en los artículos 588 ter e) 588 septies b) y 588 octies. Al tiempo hay que tener especialmente en cuenta las mayores barreras a la investigación de la nube que imponen las empresas a través de la encriptación como reacción al caso *Snowden*.

[7] Así, GRUPO DEL ARTÍCULO 29, *Dictamen 05/2012*, pág. 5

[8] Así, LARRY ELLISON, CEO de Oracle en 2009 diría que "Las nubes son vapor de agua. […] Esto no es más que un ordenador conectado a una red" en Venturebeat, acceso en http://goo.gl/pCXfj2 Y un importante analista de Gartner diría el 8.10.2010 que la nube está en la cima de las "expectativas infladas". Así, en "Gartner Hype Cycle 2010: Cloud Computing at the Peak of Inflated Expectations", en *Readwrite.com*, http://goo.gl/bkwr9T

La nube supone[9] una nueva forma de prestación de los servicios de tratamiento de la información que permite al usuario no hacer inversiones de infraestructura, sino que utiliza la que pone a su disposición el prestador del servicio. Como avanzara Carr en 2005, para las corporaciones las TIC dejan de ser una propiedad, para pasar a ser un servicio que adquieren como usuarios[10]. El usuario dispone virtualmente de sus bases de datos, correo electrónico, nóminas o gestión de recursos humanos, etc. a través de internet, mientras que físicamente dicha información puede estar deslocalizada, en cualquier lugar del mundo. El mismo prestador de servicios de nube puede a su vez deslocalizar dicha información, compartiendo o subcontratando servicios en otra escala y de forma dinámica, esto es, según las necesidades. De este modo, se proporciona un servicio a demanda. Uno de los caracteres básicos del *cloud* es la optimización de la asignación y coste de los recursos a las necesidades, lo mismo que la elasticidad de los servicios de la nube y su adaptación a las necesidades específicas. El usuario externaliza sus servicios y no tiene que gestionar la infraestructura, el sistema informático sino que lo hace el prestador de servicios de nube. Al tiempo de reducir costes (locales, equipos y conocimientos informáticos, personal especializado, etc.), la eficacia del servicio está más garantizada así como la seguridad, que quedan en manos de proveedores especializados. Los prestadores, por lo general, son grandes proveedores con infraestructuras complejas, si bien también hay lugar para prestadores intermedios con servicios añadidos y personalizados.

Los servicios de la nube pueden ser variados según diversos criterios. Interesa en este sentido recordar lo que implica la nube privada, pública o híbrida. Cuando se trata de nube privada, hay una infraestructura informática dedicada exclusivamente e individualmente para su usuario. La información queda bajo el control de dicho individuo que es el responsable. La infraestructura puede ser del mismo usuario o puede tratarse de un servicio que le prestan de manera exclusiva, de modo que no participan terceros en

[9] Para una aproximación general y en especial las definiciones, se sigue: MELL (2009) ; GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012… cit. págs. 29 y ss.; ENISA (2009); AGPD (2013 a) AGPD (2013 b)

[10] CARR (2005) pág. 68.

esta relación ni se comparten los servicios de información. Es como un centro de datos convencional a distancia, si bien con la referida característica de la optimización de los recursos a las necesidades. Por el contrario, la nube pública implica que la infraestructura es del prestador de servicios. El prestador presta sus servicios de forma abierta a los distintos usuarios, entidades heterogéneas, que comparten dicha infraestructura a través de internet. Los usuarios no tienen otra relación que la de ser usuarios del servicio. El usuario transfiere en buena medida el control sobre sus datos. Hay soluciones intermedias, así, se considera nube híbrida cuando determinados servicios se ofrecen de forma pública y otros de forma privada. También se habla de “nubes comunitarias” cuando la infraestructura informática es compartida por varias organizaciones en beneficio de una comunidad de usuarios específica. Ningún proveedor de nube pública puede garantizar siempre una calidad de servicio (sobre la base de acuerdos de nivel de servicio) capaz de responder a la naturaleza crítica del servicio, por lo que organizaciones grandes o medias siempre necesitarán nube privada. Ahora bien, basarse sólo en una nube privada, aunque puede ser factible y aconsejable desde una perspectiva de seguridad y eficacia, puede no ser viable a largo plazo por razón de los costes.

Cabe también hacer referencia a los tres modelos de servicios que suelen aplicarse a las soluciones en nube, tanto públicas como privadas: Infraestructura de nube como servicio (*IaaS*), Nube de Software como servicio (*SaaS*), y Plataforma como Servicio (*PaaS*).

La infraestructura de nube como servicio (IaaS) es como el servicio en bruto de dar almacenamiento y alojamiento masivo en servidores remotos, sustituyendo a los sistemas informáticos de empresa. El usuario ha de tener sus aplicaciones. En la Nube de Software como servicio (SaaS) el usuario cuenta con aplicaciones en la nube como una aplicación de contabilidad, de correo electrónico, un *worlkflow*, un programa para la gestión documental de su empresa, hojas de cálculo, herramientas de tratamiento de textos, agendas y registros informatizados, calendarios compartidos, etc. Así, el prestador proporciona en línea distintos servicios de aplicaciones y los pone a disposición

de los usuarios finales de modo que el usuario ya no necesita contar con ellos en la organización. Una opción intermedia es la Plataforma como Servicio (PaaS), en las que se proporcionan herramientas para construir aplicaciones, como bases de datos o entornos de programación sobre las que el usuario puede desarrollar sus propias soluciones. El usuario desarrolla y aloja aplicaciones que bien destina a su organización o a terceros y, en todo caso, no necesita equipos o programas específicos o adicionales a nivel interno.

Se pueden señalar características esenciales de los servicios en la nube[11]:

- Autoservicio a la carta: el usuario se abastece unilateralmente de sus necesidades informáticas sin interacción humana.

- Amplio acceso a la red a través de diversos terminales.

- Posible uso común de recursos, asignados y reasignados dinámicamente según necesidades.

- Rapidez y elasticidad a escala de suministro de capacidades según necesidades, con redimensionamiento inmediato que llevan a que aparezcan como ilimitadas para el usuario que las puede adquirir al momento.

-Deslocalización, por cuanto se cuenta con el servicio a distancia con independencia material de dónde éste se preste.

-Servicio supervisado por el prestador de servicios que controla y optimiza el uso de recursos. El uso de recursos puede seguirse, controlarse y notificarse, lo que aporta transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

-Costes reducidos, convirtiendo gastos de capital (habitualmente inversiones grandes) en gastos de funcionamiento, de servicios, con barreras de entrada reducidas.

[11] CLOUD SECURITY ALLIANCE (CSA), (2009).

-Seguridad, en principio aumenta por la centralización de datos y concentración de las medidas de seguridad, a cargo de proveedores especializados.

La nube implica cambios sociales y económicos muy trascendentes. La empresas, desde la más grande a la más pequeña actúan en mercados abiertos y globales y lo hacen en buena medida utilizando los servicios online descritos. La mayor parte de los usuarios acceden a contenidos y aplicaciones que están o se ejecutan en la nube. El trabajo online y el "Bring Your Own Device" (*BYOD*, "trae tu propio dispositivo") se está generalizando. Alrededor de un 90% de los empleados (en los países desarrollados) utilizan sus propios dispositivos para el trabajo o acceder a distancia a la información de la empresa, con los peligros y fisuras de seguridad que ello puede generar[12]. Desde la perspectiva económica y como se recuerda desde Europa[13], el sector de las TIC es directamente responsable del 5 % del PIB europeo, con 660.000 millones de euros. Y más allá de esta cantidad, contribuye especialmente al crecimiento de la productividad general al elevado grado de dinamismo e innovación inherente al sector y a su capacidad para transformar el modo de funcionamiento de otros sectores. Así, implica un 20 % directamente del sector de las TIC y un 30 % de las inversiones en TIC). Un estudio para Microsoft[14] afirma que el *cloud computing* creará cerca de 14 millones de nuevos empleos en todo el mundo en 2015, de ellos, 134.000 corresponderían a España[15]. En nuestro país hay algunas agrupaciones sectoriales, vinculadas al ámbito europeo[16]. Otros estudios afirman la creación de hasta 800.000 empleos en

---

[12] Sobre el tema acaba de aparecer la monografía de PUYOL MONTERO (2015).

[13] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Bruselas, 26.8.2010. COM(2010) 245 final/2. Pág. 5

http://www.agendadigital.gva.es/documents/128745511/128746769/agenda-digital-europeaES.pdf/08065334-7f50-418e-a3ab-87210fc1eb85

[14] GANTZ (2012).

[15] Esta afirmación por Microsoft España en http://www.microsoft.com/spain/prensa/noticia.aspx?infoid=/2012/03/n009- *cloud*-Computing-generara-millones-de-empleos

[16] Así, en España la Agrupación " Cloud Network (http://www.agrupacion *cloud*.com/) o Euro Cloud España http://www.eurocloudspain.org, miembro de CEIM – CEOE. En el sector de la seguridad en general, cabe tener especialmente en cuenta a la Asociación Española para el Fomento de la Seguridad de la Información *ISMS Forum Spain* (https://www.ismsforum.es), con

Europa para el mismo periodo[17]. Los beneficios de la nube se estiman en 1,1 billones (europeos) de dólares[18]. Ello, y el ya comentado ahorro de costes y el aumento de la productividad que proporciona el *cloud computing*, provocará una importante reinversión por parte de las organizaciones, y por consiguiente, el crecimiento del empleo. Los poderes públicos son conscientes del potencial de la nube y así se aprecia con claridad en los objetivos en las *Agendas* digitales europea[19] y, especialmente, en la española[20]. Es más, se tiene en cuenta que una mejora del marco jurídico de protección de datos puede contribuir al desarrollo del sector[21].

1.2 La cruz: los riesgos de seguridad y privacidad

Sin perjuicio de las muchas posibles ventajas, también el uso de la nube presenta diferentes inconvenientes generales, a saber: la disponibilidad de las aplicaciones está sujeta a la disponibilidad de acceso a internet; puede darse un ambiente propicio para el monopolio y el crecimiento exagerado en los servicios; hay un avance continuo en las aplicaciones y servicios lo cual conlleva cierto lastre para el aprendizaje en empresas de orientación no tecnológica; hay riesgos de sobrecarga en los servidores de los proveedores y

---

120 empresas y más de 800 profesionales asociados. También cabe tener en cuenta la *Cloud Security Alliance (https:// cloudsecurityalliance.org)* , con *ISMS* en España tiene la iniciativa *Cloud Security Alliance* España *(CSA-ES)* que reúne a miembros representativos de la industria del *cloud* Computing en España. En este ámbito Se trata de un foro de debate que promueve el uso de buenas prácticas para garantizar la seguridad y privacidad en el entorno del *cloud* Computing y en el marco del cual se difunden estudios como el reciente ISMS -CSA-ES (2014)

[17] BERGER (2012).

[18] GANTZ... *cit*. pág. 2.

[19] COMISIÓN EUROPEA, *Una Agenda Digital para Europa*. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones,. Bruselas, 26.8.2010. COM(2010) 245 final/2, acceso en español en http://www.agendadigital.gva.es/documents/128745511/128746769/agenda-digital-europeaES.pdf/08065334-7f50-418e-a3ab-87210fc1eb85

[20] *Agenda Digital para España*, Ministerio de Industria, Energía y Turismo y por el Ministerio de Hacienda y Administraciones Públicas, Febrero de 2013. www.agendadigital.gob.es

Entre los seis grandes objetivos y en el marco del desarrollo de la economía digital (el 2, pág. 5) y se propone "potenciar el desarrollo y uso del *cloud* computing" (pág. 6). Asimismo, entre las propuestas para "Potenciar las industrias de futuro" (apdo. 2.6, págs. 28 y ss.) se considera la nube como "oportunidad industrial" y se formulan diversas propuestas concretas.

[21] Así, *ibídem*, en concreto el punto 6, apdo. 4.3, pág. 42.

la centralización de las aplicaciones y el almacenamiento de los datos origina una interdependencia de los proveedores de servicios[22].

No obstante, y por lo que aquí más interesa, un riesgo esencial es la seguridad y la privacidad. Es cierto que –como se dijo- lo servicios de la nube mejoran la seguridad y privacidad: la información no queda diluida en los numerosos usuarios responsables de ficheros no familiarizados con lo informático, la seguridad y la legalidad, sino concentrada en manos de especialistas en seguridad con grandes equipos, formación e infraestructura. No obstante, la información del usuario ya no queda localizada en la organización y bajo su control, sino que queda más o menos expuesta a terceros, ya por su acceso a las infraestructura de los prestadores de servicios de nube, ya por los riesgos de seguridad en las continuas conexiones entre el usuario y el prestador.

Los informes mundiales sobre seguridad en la nube[23] han descrito los riesgos más importantes. Las preocupaciones que derivan de estos informes se centran en aspectos de la gestión de los datos, fundamentalmente en la propiedad de los mismos y la forma de operarlos y tratarlos por parte de los proveedores, así como en la identificación y control de acceso a los recursos. El grupo del artículo 29, por ejemplo, divide los riesgos en la falta de control de los datos y la falta de transparencia: por cuanto a la falta de control, dice que se manifiesta en falta de disponibilidad, de portabilidad, de integridad, de confidencialidad, la complejidad y la dinámica de la cadena de subcontratación. Falta de aislamiento de datos de los distintos usuarios, falta de transparencia no ser conscientes de las amenazas y riesgos, la existencia de múltiples encargados del tratamiento y subcontratistas y, por último, las diferentes zonas geográficas, fuera o dentro de la Unión Europea[24].

---

[22] Estos riesgos se siguen entre otros en en *Wikipedia*, voz: “computación en la nube” http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube

[23] Como los informes elaborados por el Grupo del artículo 29, la Cloud Security Alliance (CSA), Gartner o, en España, Inteco ya citados o que se citan a continuación.

[24] GRUPO DEL ARTÍCULO 29, “Dictamen 05/2012… cit. pág. 6 y ss.

La *Cloud Security Alliance* (CSA) señala como amenazas el abuso y mal uso del *cloud computing* (especialmente en servicios *IaaS* y *PaaS* – infraestructura y plataforma como servicio*);* el uso de interfaces y *API (Application Programming Interface)* poco seguros, que son los que sirven para que el usuario controle e interactúe con los recursos contratados. Recuerda la CSA que la autenticación, acceso, cifrado de datos, etc. del usuario se realiza a través de estas herramientas y pueden generar problemas de seguridad tanto intencionados como forma accidental.

En cualquier caso, se insiste en que la amenaza interna es una de las más importantes, esto es, el riesgo que procede del prestador de servicios de la nube, puesto que tiene acceso de forma natural a los datos y aplicaciones de la empresa. También se insiste en los problemas derivados de las tecnologías compartidas, dado que los componentes físicos, el hardware, no fueron diseñados para una arquitectura de aplicaciones compartidas. Asimismo, en la nube, aumenta el riesgo de la fuga de información, debido a la propia arquitectura de la misma el número de interacciones se multiplica. De igual modo, se afirman los riesgos por desconocimiento de con quién se comparte la infraestructura o los intentos de acceso no autorizados pueden resultar muy importantes a la hora de decidir la estrategia de seguridad[25].

A los anteriores riesgos y problemas, Gartner añade otros riesgos de la nube, como es el teletrabajo y acceso a datos fuera de las instalaciones de la empresa (*BYOD)*. La deslocalización de la información y el desconocimiento de dónde y en qué país están alojados los datos. También, respecto de la nube pública, se señala el riesgo que implica que varios clientes compartan la misma infraestructura, por ello, el proveedor debe garantizar el aislamiento de los datos de los respectivos clientes. De igual modo, se han señalado las dificultades que entraña la nube para la investigación de actividades ilegales, que en entornos *cloud* puede ser una actividad casi imposible, porque los datos y *logs* (registros de actividad) de múltiples clientes pueden estar juntos e incluso desperdigados. Por último, se indica el riesgo de la viabilidad a largo

[25] Estos riesgos son los reflejados por CLOUD SECURITY ALLIANCE, (2010).

plazo, puesto que el mercado es cambiante y cabe la posibilidad de que el proveedor sea comprado o absorbido por alguno con mayores recursos[26].

En España y a la vista de estos problemas, INTECO ha insistido en las claves de garantizar que los datos están almacenados de forma segura y aislados, pese a que se comparta la infraestructura y sistemas con otros clientes del servicio de la nube. De ahí la importancia de la autenticación de identidad de los usuarios y la eficaz eliminación o saneamiento de datos cuando corresponde, por el riesgo también de los recursos compartidos. Asimismo se recuerdan las amenazas de ataques de denegación de servicio, fallos del equipamiento y desastres naturales que amenazan la disponibilidad de la información por el usuario. Y para ello, es esencial que el prestador de servicios dé respuesta a los incidentes de seguridad, esto es, la verificación, el análisis del ataque, la contención, la recolección de evidencias, la aplicación de remedios y la restauración del servicio[27].

Como recuerda la CSA, el objetivo, al fin y al cabo, es garantizar el ciclo de vida de la seguridad de la información, que consiste en seis fases: creación, almacenamiento, uso, compartición (hacer accesible la información a otros), archivo a largo plazo y, por último, destrucción. Y en la nube los retos clave al respecto se centran en[28]: (1) la geo-localización de los datos. Debe existir una garantía de que los datos estén donde legalmente sea posible. (2) Garantizar que los datos sean eliminados de manera efectiva y completa cuando se considere que son "destruidos". (3) Que no se mezclen –especialmente los datos sensibles- con datos de otros clientes en su uso, almacenamiento o tránsito. Y (4), garantías de recuperación y restauración de datos con planes efectivos de backup frente reescritura de datos o destrucción. Pues bien, lo que aquí se sostiene es que el ámbito de la legalidad y privacidad se inserte en el ciclo de vida de la seguridad de la información. Como recientemente ha

[26] GARTNER (2011).

[27] INTECO-CERT, (2011) págs. 24 y ss.

[28] Se sigue de CLOUD SECURITY ALLIANCE (CSA), *Guía para la Seguridad … cit.* en cocreto, cap. 5, "Gestión del ciclo de vida de la información", por Geir Arild Engh-Hellesvik, Wing Ko, Sergio Loureiro, Jesus Luna, Rich Mogull, Jeff Reich, págs. 21 y ss.

señalado Martínez[29], tras la primera fase de expansión y generalización de los servicios de la nube y su significativa reducción de costes, hay que esperar la madurez de un mercado que debe exigir seguridad, privacidad y cumplimiento de la legalidad, cuestión a la que ahora se dedica la atención.

2. Los sujetos y la regulación actual y futura de la protección de datos en la nube

2.1 Quién es quién en la nube a los efectos de la normativa de protección de datos

A los efectos de la normativa de protección de datos, es bien relevante determinar quién es quién en la prestación de servicios de la nube. Se trata de una cuestión inicialmente compleja[30], sobre la que hoy hay bastante claridad. Pues bien, como ha recordado el Grupo del artículo 29[31] y la Agencia Española de Protección de Datos (AEPD)[32], el prestador de servicios de nube es, en términos del art. 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), un "encargado" del tratamiento de datos, que actúa para la organización cliente del servicio en la nube contratado. Y el usuario o cliente es, en términos de legislación de datos, el "responsable" de dicho tratamiento (quien decide sobre la finalidad, contenido y uso del tratamiento). El "responsable" al fin y al cabo es quien decide la contratación de dichos servicios, el mantenimiento o no de sus propios sistemas de información, la modalidad de nube y la tipología de servicios que contrata y la elección del proveedor. Y esta responsabilidad de quien utiliza servicios de la nube, al derivarse de la aplicación de la ley, no puede alterarse contractualmente[33]. No obstante, el marco contractual como luego se aprecia, es clave para la definición de papeles y es prueba objetiva de

[29] MARTÍNEZ i MARTÍNEZ (2014).
[30] Así, dedica buena parte del mismo a esta cuestión LEENES, Ronald (2010).
[31] GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012… cit.
[32] Tanto en AGPD, *Guía* como en AGPD, *Orientaciones* (2013).
[33] AGPD, *Orientaciones para prestadores… cit.*

la diligencia de las partes, así como juega un papel básico para la legalidad de las transferencias de datos internacionales.

Aunque no necesariamente en todos los casos, el encargado, esto es, la empresa que presta servicios de la nube, normalmente será una gran corporación que cuenta con una posición prevalente en la contratación. De ahí que quien contrata servicios de la nube queda en una posición compleja por cuanto es "responsable" y la posición prevalente del prestador de servicios –encargado del tratamiento- puede ser un obstáculo para cumplir sus obligaciones. El futuro reglamento europeo de protección de datos en la línea de lo afirmado por el Grupo del artículo 29 de la UE, busca equilibrar la asimetría que puede producirse por esta preeminencia de los prestadores de servicios de la nube y sus usuarios. [34]

2.2 Las cuestiones clave de protección de datos y las insuficiencias de la regulación actual

Como desde sus inicios puso en evidencia la Declaración de Independencia del Ciberespacio de 1996[35], no son pocos los problemas que implica en general la regulación de internet[36]. Y la regulación de la nube no es en modo alguno ajena a estos problemas. En el ámbito de la nube, Reed[37] ha insistido recientemente en modelos de co-regulación trasnacional, en especial se insiste en que es necesario reforzar la legitimación de las normas. Y tal legitimación debe venir de la mano de un *regulador nebuloso* ("cloud-regulator") que genere las normas con la participación de la comunidad afectada (instituciones, individuos y las entidades empresariales implicadas), pero que

[34] GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012… cit.

[35] Redactada por John Perry Barlow, Fundador de Free, Fronteras Electrónicas en Davos (Suiza) el 8 de febrero de 1996. http://www.internautas.org/documentos/decla_inde.htm

[36] Sobre la problemática de la regulación de la red, referencia obligada LESSIG (2001) Y en español MUÑOZ MACHADO (2000. En general y más actual es la reflexión de Reed (2012) capítulo 4.

[37] REED (2013). , Acceso en SSRN y cloudlegalproject.org

sea aceptada por los Estados e instituciones, que tienen que hacer valer tales normas.

Aunque no de manera exclusiva, el fenómeno de la nube atrae la cuestión de la protección de datos[38], que es la que centra mayormente aquí el interés. Y en materia de protección de datos, la ley aplicable es la del lugar del cliente de servicios de la nube[39], quien como se ha expuesto *supra*, es el responsable del tratamiento. Así pues, al usuario de servicios de la nube se le aplicará su ley nacional y, en consecuencia, el centro de atención es la Directiva 95/46/CE sobre protección de datos y, obviamente para España su transposición a través de la LOPD y su desarrollo reglamentario. También habrá que seguir la Directiva 2002/58/CE (modificada por la Directiva 2009/136/CE)[40].

Miralles[41] ha sintetizado los aspectos más relevantes del nexo de la protección de datos y el *cloud* computing: 1) La pérdida de control sobre el tratamiento de la información, tanto por parte de las personas afectadas como por parte del responsable del tratamiento, y las consecuencias que se puedan derivar de ello (seguridad, confidencialidad, ejercicio de derechos, etc.); 2) Las dificultades de encajar jurídicamente y con suficiente agilidad las situaciones de tratamiento de los datos por cuenta de terceros: el encargado del tratamiento *cloud* y las posibles subcontrataciones. 3) Las problemáticas derivadas del movimiento internacional de datos. 4) Y, por último, la resolución efectiva de los incidentes relacionados con la vulneración del derecho fundamental en la protección de datos personales en situaciones de multiterritorialidad.

Frente a estos retos principales que con más detalle se analizan *infra*, no son pocas las disparidades y posibles choques entre normativa americana y

---

[38] Además de los estudios que se de modo más concreto, un análisis general de la cuestión, FERNÁNDEZ-ALLER (2012). También, una aproximación general, GARCÍA MEXÍA (2010).

[39] Así en especial GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012… cit. pág. 8 y Dictamen 8/2010 sobre la ley aplicable http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf

[40] Dicha norma respecto de la confidencialidad de las comunicaciones y del tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas en las redes públicas de comunicaciones (operadores de telecomunicaciones), si tales servicios se prestan a través de soluciones en la nube, lo cual no es extraño.

[41] MARTÍN MIRALLES (2010).

europea de protección de datos para la nube[42]. Como especialmente recuerda Marzo para la nube, la Directiva 95/46/CE está muy desfasada y se ha convertido en una traba para las relaciones entre Europa y los terceros países. Como luego se aprecia, el Grupo del Artículo 29 y la AEPD han sido proactivos en los últimos años para colmar las lagunas e incertidumbres de una normativa no concebida para la nube. En todo caso, dado que las empresas y administraciones públicas españolas no pueden abandonar el barco del "progreso tecnológico" [43], necesariamente tienen que arriesgarse a contratar servicios de *cloud* computing sin un marco jurídico adecuado. La rigidez normativa sitúa a Europa y a su industria en una posición de clara desventaja competitiva frente al desarrollo de modelos de negocio de nube por la industria de los terceros países. La alternativa, obviamente, es desarrollar grandes plataformas de *cloud* europeas respetuosas de las garantías europeas. Y no parece que pueda aventurarse este futuro.

2.3 La nube en el esperado Reglamento europeo de protección de datos. Hacia una regulación nebulosa

Como es sabido, desde enero de 2012 se maneja el texto de un futuro Reglamento europeo de protección de datos del que hay diversas versiones y parece ser que se aprobará en 2016. Aunque lamentablemente no hay referencia expresa a los servicios de la nube, obviamente la regulación proyectada se proyecta para el *cloud computing*[44]. Entre otros aspectos, el Reglamento destaca por la figura del delegado de protección de datos (DPO, *data protection officer*, arts. 35-37). Dicha persona, en nuestro caso, de la empresa cliente que contrata servicios de la nube, habrá de asumir el conocimiento y decisiones en la materia. A este respecto, la empresa que provee servicios de la nube también deberá de generar todas unas buenas

---

[42] Un análisis concreto sobre disparidades y posibles choques entre normativa americana y europea de protección de datos para la nube, SCHWARTZ, (2013).

[43] MARZO PORTERA (2012) pág. 225.

[44] HON, W. Kuan y otros. *(*2014) HON, W. Kuan y otros (2015). En español, sobre el futuro reglamento hay un amplio comentario de 500 págs. de SEMPERE SAMANIEGO (2014).

prácticas y trasparencia sobre su actuación para facilitar la actividad y carga de responsabilidad del DPO.

También y especialmente, en razón del futuro Reglamento europeo puede tener mucha proyección en el ámbito de la nube la exigencia de la privacidad por diseño y por defecto[45]: "El principio de protección de datos desde el diseño requiere la integración de la protección de datos en todo el ciclo de vida de la tecnología, desde la primera fase de diseño hasta su despliegue final, su utilización y su eliminación definitiva. Debe abarcar asimismo la responsabilidad por los productos y servicios utilizados por el responsable o el encargado del tratamiento. El principio de protección de datos por defecto exige que la configuración de la privacidad de los servicios y productos cumpla por defecto los principios generales de protección de datos, como la minimización de los datos y la limitación de los fines."[46] También y para estimular el cumplimiento, se prevé que estas exigencias de privacidad por defecto y en el diseño que pasen a ser "un requisito previo para las licitaciones de contratos públicos" (art. 23. 1 bis, versión marzo 2014). No obstante, tras casi cuatro años desde el primer texto conocido, habrá que ver la regulación final que en su caso se apruebe.

Y además de la regulación ya contenida en el futuro artículo 23, puede pensarse que ésta se concretará y de manera mucho más precisa a través actos delegados y normas técnicas por parte de la Comisión Europea que están previstos (art. 23. 2º y 3º y art. 86). Puede así esperarse que en unos años diversos servicios de la nube pasen a ser un sector bastante regulado. Ahora bien, no hay que obviar el cumplimiento de modelos y esquemas de certificación específicos para los entornos de nube facilita y garantiza la elección del proveedor por el cliente. En este punto, dentro de las normas ISO 27000 de seguridad de la información, es especialmente destacable la muy

[45] En general cabe seguir el término y desarrollo por Anna Cavoukian, entonces Comisionada de Información y Privacidad de la Autoridad de Protección de Datos de Ontario (Canadá). De referencia, el Centro de Investigación impulsado por ella http://www.privacybydesign.ca/

[46] Considerando 61 en la versión de marzo de 2014 por el Parlamento Europeo. *Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento.*

reciente ISO/IEC 27018:2014 de 27 de julio de 2014[47] de seguridad en la nube. Se hace difícil pensar que la futura normativa técnica que haga la Comisión Europea en razón sus competencias ejecutivas en del desarrollo del futuro Reglamento europeo no tengan una conexión con la normativa técnica privada.

Como se ha señalado, muy posiblemente cuando se desarrolle esta normativa técnica (pública, claro está), habrá de tenerse en cuenta los usos, prácticas y autorregulación técnica ya consolidados en el sector. De ahí es posible que resulte la *regulación nebulosa* ("cloud regulation"), la co-regulación trasnacional del sector con ciertas garantías de exigibilidad y cumplimiento.

3. El tratamiento jurídico de algunas cuestiones clave que plantea la nube en materia de protección de datos

3.1 La diligencia y responsabilidad legales del usuario de la nube, transparencia de la empresa de cloud

Según se ha señalado, el cliente de servicios de la nube es "responsable" de protección de datos y la empresa proveedora de servicios, "encargado". El usuario de nube como responsable tiene obligación legal de diligencia para "velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto" en la normativa de protección de datos personales (art. 20.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, RLOPD). El usuario de nube –responsable LOPD- debe hacer una ponderación de riesgos a partir de toda la información que sea posible. La AGPD ha adoptado un papel activo para difundir el conocimiento de esta responsabilidad y de los elementos de juicio para tomar decisiones[48]. Así, por ejemplo, ha señalado las preguntas que

[47] "Tecnología de la información - Técnicas de seguridad - Código de conducta para la protección de la información de identificación personal (PII) en nubes públicas que actúan como procesadores PII".

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498

En español, sobre esta nueva norma técnica, una descripción http://blog.segu-info.com.ar/2013/06/iso-27017-iso-27018-e-iso-27036-guias.html

[48] AGPD, *Guía* (2013).

debe formularse la empresa o Administración (a través del futuro delegado de protección de datos) antes de contratar servicios de nube.

Y para poder desarrollar esta labor por el responsable, es esencial la transparencia por parte de la empresa prestadora de servicios de la nube. Como han señalado las instituciones y autoridades de protección de datos, la transparencia es "un principio esencial que debe presidir las relaciones entre las partes, especialmente en los casos en que el proveedor de servicios ocupa una posición preeminente sobre los clientes" [49] (especialmente PYMES, microempresas, profesionales o Administraciones públicas sin gran estructura orgánica). Esta diligencia se traduce en exigencias importantes de transparencia al prestador de servicios para conocer sus garantías y si cumple lo exigible por la normativa y tomar las decisiones. El prestador de servicios de nube debe informar a los clientes de todos los subcontratistas de los respectivos servicios en nube y de todos los lugares donde los datos puedan ser almacenados, en especial, los lugares fuera del Espacio Económico Europeo-EEE). También el cliente deberá disponer de información significativa sobre las medidas técnicas y de organización aplicadas por el proveedor[50].

Y como señala el Grupo del Artículo 29 de la UE[51], respecto del futuro Reglamento europeo, la empresa de *cloud* (encargado del tratamiento) que no se atenga a las instrucciones del responsable del tratamiento, será considerado responsable del tratamiento y estará sujeto a las normas específicas en materia de control conjunto. Ello se realiza precisamente para equilibrar la situación habitual de preeminencia del prestador de servicios de la nube respecto del usuario, responsable del tratamiento, especialmente si se trata de una PYME.

A estas obligaciones de la empresa que presta servicios de nube[52], hay que sumar tradicionales exigencias a un encargado que aloja datos[53]. Y cabe

[49] AGPD, *Orientaciones* (2013).

[50] GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012… cit. Ver apartado 3.4.1.1 pág. 18

[51] *Ibídem*, págs. 26 y ss.

[52] Cabe destacar el reciente estudio AAVV. ENATIC, (2014). Ahí se analiza la responsabilidad de la empresa atacada, ya como cliente, ya como proveedora de servicios de las responsabilidades.

recordar en este sentido que han de venir recogidas en contrato (art. 12 LOPD). Entre tales obligaciones, una vez acabe la relación contractual, está la destrucción, devolución de los datos al responsable o su transferencia a la nueva empresa contratada (art. 12. 2º y 3º LOPD y art. 22 RLOPD). En una versión inicial del Reglamento europeo de protección de datos, se incluyó un derecho a la portabilidad que, no obstante, ya no se ha incluído en versiones posteriores. Y en cuanto a las medidas de seguridad que ha de cumplir la empresa de la nube, serán "las mismas que las impuestas al responsable del fichero" (arts. 9 y 12.2 de la LOPD)[54]. En este sentido cabe recordar que el artículo 81. 8º RLOPD permite aplicar diferentes niveles de seguridad a un fichero. Asimismo, el encargado del tratamiento debe de elaborar el correspondiente documento de seguridad (art. 82.2º RLOPD).

Por lo expuesto y en la práctica, tendrá un especial interés comprobar las relaciones reales de la empresa de servicios de la nube con los clientes según sus perfiles. En este sentido cabrá prestar atención al papel activo de empresa y clientes en la definición del lugar que les corresponde como encargado y responsable de tratamiento. Asimismo, será de especial interés para la potenciación de los servicios de la nube descubrir las mejores prácticas para que la relación sea equilibrada entre uno y otro y tendente a la confianza y al mejor cumplimiento de las exigencias de seguridad y legales. Sin duda y en la práctica, es clave el papel pedagógico de la empresa de servicios de la nube y su proactividad en la difusión de información en incluso formación para sus clientes.

3.2 Un elemento clave para el cliente y la empresa de cloud: el conjunto contractual y la subcontratación

El contrato es la expresión de la relación jurídica entre el cliente –responsable- y el proveedor de servicios de la nube –encargado y su existencia

---

[53] En particular recogidas en el Informe 574/2009 de la AEPD sobre Carácter de encargado del tratamiento de un prestador de servicios de alojamiento (acceso en web AEPC).

[54] *Ibídem*, en el mismo sentido Informe 620/2009.

y unos contenidos mínimos se derivan del artículo 12 LOPD. Más allá de la exigencia formal, el contrato entre el encargado y el responsable es un indicador de la diligencia y responsabilidad del usuario de la nube (responsable). Pese a ser una responsabilidad del cliente, el "responsable", en la práctica y realidad de la nube, la empresa de servicios de la nube (encargado) debe tener preparado un cuerpo contractual fuerte para dar toda la confianza y seguridad jurídica a sus clientes (responsables). Dicho cuerpo contractual normalmente se instrumenta por el contrato particular, que remite a unas condiciones generales de contratación que, a su vez, habitualmente remiten a un documento técnico de "Acuerdo de Nivel de Servicio". También en los casos de consumidores, pueden ser relevantes jurídicamente los folletos o información comercial que haya accedido el cliente. Todo este conjunto contractual juega un papel clave en los servicios de la nube como garantía no sólo de las partes, sino del cumplimiento de la legalidad y la seguridad jurídica.

Además, y como es más que habitual en los servicios de nube, intervendrán empresas subcontratadas[55], es decir, el proveedor de nube empleará a su vez otros servicios de nube para realizar su prestación como socios, *partners, resellers*, *cloud builders* etc. Y en este caso la normativa (en especial el artículo 21. 2º RLOPD) exige mayores garantías, como ha ratificado la STS de 15 de julio de 2010, FJ 10º[56]. Así, las garantías deben darlas los socios de prestadores de nube, en cualquiera de las figuras de *reseller*, agregadores de servicios de *cloud*, *cloud builders*, proveedores de aplicaciones, etc., y que proporcionan servicios contratando directamente con los clientes.

[55] Entre otros, dedica alguna atención a las subcontrataciones FERNÁNDEZ-ALLER, Celia, "Algunos retos… cit. págs. 137-138

[56] En el recurso de legalidad frente a este precepto, que es desestimado y se da por buena la obligación de que el encargado del tratamiento comunique al responsable la necesidad de subcontratar y con quién pretende hacerlo. Tanto en AGPD, *Guía para clientes … cit.* como en AGPD, *Orientaciones para prestadores… cit.* se recuerda que se exige*:"* La identificación de los servicios y la empresa a subcontratar informando de ello al cliente (incluido el país en el que desarrolla sus servicios si están previstas transferencias internacionales de datos). Que el cliente pueda tomar decisiones como consecuencia de la intervención de subcontratistas y la celebración de un contrato entre el prestador de servicios de *cloud* computing y los subcontratistas con garantías equivalentes a las incluidas en el contrato con el cliente."

El Grupo del artículo 29 ha recordado diversos contenidos y garantías en el contrato de servicios de nube[57], los mismos tiene su reflejo en la guía de la AEPD para los clientes de servicios[58]. Y hay que buscar un cuerpo contractual equilibrado entre las responsabilidades de cliente (responsable del tratamiento) y empresa de nube (encargada del tratamiento)[59].

-Entre ellos está la mencionada garantía de la portabilidad, esto es, que al concluir el servicio, los datos se devuelvan al cliente o se transfieran a un nuevo proveedor de nube tras el contrato.

-También debe recogerse claramente la obligación para el proveedor de nombrar a todos los subcontratistas contratados [60]. Se recogerá que el proveedor hará públicos todos sus subcontratistas, por ejemplo a través de un registro digital público. Y a este respecto debe garantizarse que el cliente conozca cualquier cambio por si quiere oponerse al mismo o rescindir el contrato[61].

-También ha de tener garantías efectivas frente a una posible infracción del contrato por el proveedor[62].

-El contrato debe determinar medidas de seguridad técnica y de organización (en virtud del artículo 17, apartado 2, de la Directiva).

-De igual modo [63], debe especificar las instrucciones del cliente al proveedor e incluir el objeto y el calendario del servicio, niveles de servicio objetivos y mensurables y las sanciones correspondientes (financieras o de otro tipo).

-Deberá asimismo precisar las medidas de seguridad que deben respetarse, en función de los riesgos del tratamiento y de la naturaleza de los

---

[57] GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012… cit. págs. 9 y ss. y 14 y ss.

[58] AGPD, *Guía (2013).*

[59] Un análisis de de los contratos, BRADSHAW Y OTROS (2010).

[60] GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012… cit. págs. 9 y ss. Como se ha señalado, obligación confirmada por la STS de 15 de julio de 2010, FJ 10º.

[61] *Ibídem*, págs. 23 y ss.

[62] *Ibídem* punto 3.3.2 pág. 11.

[63] *Ibídem*. 23 y ss.

datos, en consonancia con los requisitos correspondientes y con sujeción a las medidas más estrictas previstas en la legislación nacional de los clientes.

-Habrá se indicarse que sólo las personas autorizadas deberán tener acceso a los datos, con una cláusula de confidencialidad por lo que respecta al proveedor y sus empleados.

-El contrato también deberá exigir al proveedor que notifique toda solicitud jurídicamente vinculante de divulgar datos personales presentada por las autoridades policiales o judiciales a menos que dicha divulgación esté prohibida por otras razones. El cliente deberá garantizar que el proveedor rechazará cualquier solicitud de divulgación jurídicamente no vinculante.

-También se recomienda que contractualmente el proveedor de servicios coopere con el responsable del fichero, el cliente, para controlar el tratamiento y facilitar el ejercicio por los interesados de sus derechos a acceder, corregir o suprimir sus datos (ARCO).

-De igual modo, contractualmente debe reforzarse la obligación del proveedor de que se notifique al cliente toda violación de seguridad para que éste, a su vez, cumpla con la obligación legal de notificar violaciones a sus clientes.

-El contrato deberá reflejar que el cliente pueda auditar y solicitar el registro de las operaciones de tratamiento realizadas por el proveedor y sus subcontratistas. Para ello, no obstante, la mejor práctica es que contractualmente se acepten certificaciones y auditorías de terceros con plena transparencia. Así, el contrato puede reflejar la validez de tales auditorías y la facilitación de copia de la misma al cliente.

-El contrato siempre remitirá a garantías del nivel de prestación de servicios que impliquen el estándar de garantía de la disponibilidad, integridad, confidencialidad, aislamiento, posibilidad de intervención y portabilidad[64].

[64] *Ibídem* pág. 16.

No hay que olvidar que no sólo están en juego los derechos e intereses de las partes, sino la garantía de un derecho fundamental de muchos sujetos afectados que pueden quedar afectados por estar sus datos personales e información en juego.

3.3 La cobertura legal de las transferencias internacionales de las empresas de cloud contratadas y subcontratadas: cláusulas contractuales tipo y normas corporativas vinculantes

Casi por defecto, el uso de nube implica el trasiego internacional de datos[65], bien porque el prestador de servicios esté en el extranjero, bien porque, como se ha indicado, lo natural en la nube es la subcontratación de servicios por los prestadores de servicios. El marco normativo y las instituciones deben adaptarse a esta realidad al tiempo de garantizar la seguridad, privacidad y el cumplimiento de la legalidad permitiendo tales las transferencias internacionales de datos. Y debe permitirse las mismas al tiempo de asegurar que el responsable, esto es, el cliente, sigue manteniendo la capacidad de tomar decisiones.

Los datos fácilmente no estarán en España ni en territorio europeo y es posible que el los datos o el prestador estén en países terceros que no cuenten con un nivel adecuado de protección de datos (Suiza, Canadá, Argentina, Guernsey, Isla , Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y ciertas compañías estadounidenses)[66]. En tales casos, por principio es

---

[65] Sobre el tema, cabe seguir el AEPD Informe 2001-0000, *Transferencias Internacionales de datos para la realización de un tratamiento por cuenta del responsable del fichero*. Acceso en web AEPD. En la doctrina en general MARZO PORTERA y ORTEGA GIMÉNEZ, (2013), autores de dos tesis doctorales sobre el tema. De un lado, GUASCH PORTA (2012). Asimismo, la premiada tesis doctoral ORTEGA GIMÉNEZ (2014).

[66] Respecto de estos países hay Decisiones de la Comisión europea desde 2000 en las que se expresa que sí que reúnen garantías similares, a saber:

- Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.
- Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001.
- Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.
- Guernsey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003.
- Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004.

requisito una autorización del Director de la AGPD para permitir la transferencia internacional de datos (art. 33 LOPD). Y el incumplimiento de esta obligación es falta muy grave (artículo 44.4 d) LOPD).

Ahora bien, tal autorización resultará automática si se siguen las cláusulas contractuales tipo de la Comisión Europea (artículo 26.2º de la Directiva 95/46/CE de protección de datos)[67]. Así, cabe seguir especialmente la Decisión 2010/87/UE, (DOUE L 39 de 12 de febrero de 2010), centrada en la subcontratación por un encargado del tratamiento establecido en un tercer país, de sus servicios de tratamiento a un subencargado establecido en un tercer país. Como se dijo respecto del contrato, éste debe estipular de modo concreto cómo el prestador de servicios ha de aplicar los principios de la protección de datos, al tiempo de ofrecer un nivel de cumplimiento de las normas, facilitar su cumplimiento a las partes y dar vías de recurso y garantías a los perjudicados para ello.

Por su parte y de forma paralela, la AEPD elaboró en 2012 un nuevo conjunto de cláusulas contractuales para facilitar la subcontratación que ha de preverse en el contrato[68]. Se necesitan determinadas adaptaciones del entorno de la nube (para evitar tener diferentes contratos por cliente entre un proveedor y sus subencargados) lo que podría implicar la necesidad de una autorización

---

- Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008.
- Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.
- Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.
- Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.
- Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.
- Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.

Además, es singular y central el caso de EEUU, dado que se considera que sí que cumple el nivel adecuado respecto de las entidades que cumplen con los principios de puerto seguro "safe harbour". Así, decisión de la Comisión sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, en el *DOCE* L 215, de 25 de agosto de 2000. Puede consultarse qué entidades sí que cumplen con tales principios en https://safeharbor.export.gov/list.aspx

[67] Sobre el tema, los trabajos ya referidos de Giménez y Marzo y GUASCH PORTAS, Vicente y SOLER FUENSANTA (2014). También GARCÍA DEL POYO (2012), en especial, 186 y ss.

[68] Las mismas fuero conocidas con ocasión del Expediente TI/00126/2012 en la página de la AEPD, así como la publicación oficial del «Acuerdo de Apertura del Período de Información Pública» en el BOE de 20-09-2012. El contenido es similar al de las clausulas tipo de la Comisión.

previa de la autoridad de protección de datos competente. La ventaja para las empresas de *cloud* españolas es que si se logra la autorización de transferencia de datos siguiendo estas cláusulas contractuales, no se precisa en general una ulterior si se mantiene lo establecido en el contrato. Sólo tendrán que notificar –no pedir autorización–no autorice- cada nueva transferencia internacional para que ésta quede registrada[69].

Otra vía para legalizar la transferencia internacional de datos es la adopción de reglas corporativas vinculantes. Se trata de dar respuesta a las sociedades multinacionales que deben realizar trasiego internacional de datos dentro del grupo. Así, se adoptan las normas de funcionamiento y buenas prácticas (*Binding Corporate Rules*) son aprobadas por autoridades de protección de datos y han de ser efectivamente asumidas y cumplidas por las empresa multinacional. [70] Ello puede permitir que empresas de nube puedan prestar sus servicios aprovechando la natural participación de otras empresas subcontratadas de fuera de la Unión Europea.

4. Algunas exigencias del uso de la nube por las administraciones

Son diversos los retos técnicos[71] y, por lo que aquí interesa, jurídicos que suscita el uso de la nube por las administraciones[72]. Si la Administración externaliza servicios en la *nube*, tendrá que asegurarse de que de las entidades con las que contrate cumplen requisitos normativos. Y lo mejor será asegurar la expresión de estas obligaciones en los pliegos de cláusulas

---

[69] Entre otros, lo explican GUASCH PORTAS, Vicente y SOLER FUENSANTA José Ramón, "Cloud computing… cit. págs. 263 y ss.

[70] Al respecto, ver GRUPO DEL ARTÍCULO 29, "Dictamen 05/2012… cit. pág. 22 así como Comisión Europea, "Un enfoque global de la protección de los datos personales en la Unión Europea", Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones Bruselas, 4.11.2010, COM(2010) 609 final.

[71] Al respecto, en especial, CATTEDDU, (2011) 2011 en http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/es_governmental_clouds_enisa.pdf

[72] La cuestión ha sido estudiada esencialmente por VALERO TORRIJOS (2012), quien remite también a PAQUETTE, S., JAEGER, P.T. y WILSON, S.C.

administrativas generales (art. 98 Ley 30/2007, de 30 de octubre), de cláusulas administrativas particulares (art. 99) y en su caso, los pliegos de prescripciones técnicas (art. 100).

Aunque actualmente no lo hace, la ley habría de expresar la prohibición de externalización en supuestos específicos en razón de una mayor exigencia de confidencialidad y seguridad e incluso establecer determinadas garantías al prestador en casos determinados.

Una cautela esencial del prestador de servicios de la nube es evitar que la información pública en la nube no pueda verse alterada. La falla de seguridad o que la información quede fuera de control, como es obvio y recuerda Catteddu [73], puede poner en compromiso la soberanía y control gubernamentales sobre la información y los datos.

Más allá de las obligaciones dimanantes de la normativa de protección de datos que se aplica a las administraciones, en razón de la normativa de gobierno electrónico, la Administración pública habrá de confirmar las versiones de la información o documentación que en su caso genere la entidad prestataria de los servicios en la nube. Asímismo y especialmente la entidad prestadora de nube tendrá que asegurar "la identificación de los usuarios y el control de accesos" (art. 31. 3º Ley 11/2007). También y si es necesario, habrá de integrar la referencia temporal de la información o documentacion (art. 29 Ley 11/2007). Tales acciones habrán de satisfacerse por el prestador de servicios y no sólo frente a la Administración contratante, sino también de cara a las otras administraciones con las que la Administración haya de compartir información.

Además de las obligaciones de seguridad de la información en razón de la normativa de protección de datos y del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, es fundamental el cumplimiento de la interoperabilidad , y cumplir sus detalladas normas para, entre otros, garantizar la eficaz conexión de la información en la nube con otras

[73] CATTEDDU, D.D. *Seguridad y Resistencia… cit. pág. 41.*

entidades públicas o privadas (art. 8. 1 ENI). El contrato o la relación jurídica con la empresa de nube habrá de reflejar estas exigencias.

Por cuanto a la conexión entre el uso público de la nube y la actuación automatizada , en España desde la Ley 11/2007 desapareció la anterior obligación por la que las Administraciones habían de aprobar previamente las aplicaciones (antiguo art. 45.4 de la Ley 30/1992). Desde entonces sólo recae la obligación para la Administración General del Estado de que se establezcan previamente el "órgano u órganos competentes para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente" (art. 39 LAE). Así pues al menos se pretende asegurar que las decisiones administrativas al rspecto siguen criterios previos. De igual modo, la actuación automatizada en la nube requerirá de sistemas de firma electrónica. Dado que la prestación de servicios en la nube es bien posible que sea a través de una empresa habrá que extremar la precaución para evitar el uso indebido de la actuación automatizada por parte de la entidad o su personal.

Finalmente cabe plantearse con Valero el juego de responsabilidades por daños y perjuicios por una mala nube pública prestada por una empresa privada. En este supuesto, el artículo 198 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, será "obligación del contratista indemnizar todos los daños y perjuicios" a terceros en la ejecución del contrato. Pero la responsabilidad será de la Administración si ésta "hubiere impuesto ciertas condiciones que motivaran la producción del daño". Obviamente la responsabilidad variará según se los diferentes servicios de nube: por el funcionamiento de la infraestructura (IaaS), plataforma (PaaS) o aplicaciones de servicios de nube (SaaS). Y, como señala Cattedu[74], van a desempeñar un papel fundamental en este tema, de un lado, los acuerdos de nivel de servicio (ANS) detallados, que especifican los niveles de funcionamiento del proveedor de servicios en la nube y, del otro, las cláusulas contractuales que asignan derechos obligaciones.

[74] *Ibídem pág. 46.*

Bibliografía:

AAVV. *La responsabilidad legal de las empresas frente a un ciberataque*, ISMS Forum, ENATIC, Abogacía Española, Inteco, 2014. https://www.ismsforum.es/ficheros/descargas/la-responsabilidad-legal-de-las-empresas-fente.pdf

AEPD Informe 2001-0000, *Transferencias Internacionales de datos para la realización de un tratamiento por cuenta del responsable del fichero*. Acceso en web AEPD.

AEPD, *Guía para clientes que contraten servicios de cloud Computing*, Agencia Española de Protección de Datos, 2013, acceso en www.agpd.es

AEPD, *Orientaciones para prestadores de servicios de cloud computing*, Agencia Española de Protección de Datos, 2013, acceso en www.agpd.es

Agenda Digital para España, Ministerio de Industria, Energía y Turismo y por el Ministerio de Hacienda y Administraciones Públicas, Febrero de 2013. www.agendadigital.gob.es

BERGER, Roland. *La supervivencia del más apto: Cómo puede Europa asumir un papel de liderazgo en la nube*, SAP, 2012.

BRADSHAW, Simon; MILLARD, Christopher y WALDEN Ian. *Contracts for clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing* Services, Queen Mary University of London, Paper No. 63/2010. Acceso en SSRN.

CARR, Nicholas. "The End of Corporate Computing", en *MIT Sloan Management Review,* vol 47. Nº 3, de abril del 2005, págs. 67-73. Acceso en SSRN.

CARR, Nicholas. *The Big Switch: Rewiring the World, from Edison to Google, Wall Street Journal,* 2008. Acceso en SSRN.

CATTEDDU, D.D. *Seguridad y Resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones*. ENISA, 2011, http://goo.gl/5AQLKK

CLOUD SECURITY ALLIANCE (CSA). *Guía para la Seguridad en áreas críticas de atención en cloud Computing*, Resumen ejecutivo. Versión 2, noviembre de 2009, del original *Security Guidance for Critical Areas of Focus in cloud Computing V2 ,* CSA, 2009. (trad. Por ISMS Forum).

CLOUD SECURITY ALLIANCE (CSA). *Top Threats to cloud Computing V1.0*, *cloud* Security Alliance marzo de 2010, disponible en la red.

COMISIÓN EUROPEA, *Una Agenda Digital para Europa*. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones,. Bruselas, 26.8.2010. COM(2010) 245 final/2, acceso en español en http://goo.gl/kuAlyQ

COMISIÓN EUROPEA, *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones*, Bruselas, 26.8.2010. COM(2010) 245 final/2. Pág. 5 http://goo.gl/iPgw6r

ENISA " Cloud Computing: Benefits, risks and recommendations for information security" (Computación en nube: ventajas, riesgos y recomendaciones para la seguridad de la información) en: https://goo.gl/0B4MQ7

FERNÁNDEZ-ALLER, Celia, "Algunos retos de la protección de datos en la sociedad del conocimiento. Especial detenimiento en la computación en nube ("cloud

computing)", *RDUNED. Revista de derecho UNED*, nº. 10, 2012, págs. 125-145 Acceso en Dialnet.

GANTZ, John F., MINTON, Stephen y TONCHEVA, Anna. *Whitepaper. cloud Computing's Role in Job Creation*, marzo de 2012, Framingham (EEUU), dato en la pág. 2. Acceso en http://goo.gl/HLdpnC

GARCÍA DEL POYO VIZCAYA, Rafael, "La contratación empresarial de servicios de *cloud* computing", en Martínez i Martínez, Ricard, *Derecho y cloud computing*, Civitas, Cizur, 2012, págs. 179-200, en especial, 186 y ss.

GARCÍA MEXÍA, Pablo, "Cloud computing: sus implicaciones legales", *Revista Aranzadi de derecho y nuevas tecnologías*, nº. 23, 2010, págs. 79-88 .

GARCÍA MEXÍA, Pablo, *Cloud Computing. Sus Dilemas,* en la web *Legales.*

GARTNER, *Assessing the Security Risks of cloud Computing*, Stamford, Estados Unidos, 2011 acceso completo en http://goo.gl/No2K4H

GRUPO DEL ARTÍCULO 29, *Dictamen 05/2012 sobre la computación en nube*. 1 de Julio de 2012. WP196. 01037/12/ES. Dirección General de Justicia de la Comisión Europea, pág. 5 http://goo.gl/D2uae6

GRUPO DEL ARTÍCULO 29, *Dictamen 8/2010 sobre la ley aplicable* http://goo.gl/jpUdOQ

GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón. "Cloud computing, cláusulas contractuales y reglas corporativas vinculantes", en *Revista de Derecho UNED*, núm. 14, 2014, págs. 247-269.

GUASCH PORTAS, Vicente. "La transferencia internacional de datos de carácter personal" en *Revista de derecho UNED*, Nº. 11, 2012, págs. 413-454, acceso completo en Dialnet.

HON, W. Kuan y otros. *Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation*. Queen Mary School of Law Legal Studies Research Paper No. 172/2014; Acceso en SSRN.

HON, W. Kuan y otros. *Policy, Legal and Regulatory Implications of a Europe-Only Cloud*, *Research Paper 191/2015.* Acceso SSRN

Informe 574/2009 de la AEPD sobre Carácter de encargado del tratamiento de un prestador de servicios de alojamiento (acceso en web AEPC).

INTECO-CERT, *Riesgos y amenazas en cloud computing*, INTECO-CERT, marzo 2011, disponible en la red.

ISMS -CSA-ES. *Estudio del Estado de la Seguridad en Cloud Computing* https://goo.gl/7K5Ayp

LEENES, Ronald (2010). "¿Quién controla la nube?", en *VI Congreso Internet, Derecho y Política. cloud Computing: El Derecho y la Política suben a la Nube*, *IDP. Revista de Internet, Derecho y Política*. N.º 11. UOC. Acceso completo en Dialnet.

LESSIG, Lawrence., *El código y otras leyes del ciberespacio,* Taurus, Madrid, 2001.

MARTÍN MIRALLES, Ramón. "Cloud computing y protección de datos", en Cerrillo i Martínez, Agustí (coord.), *IDP: revista de Internet*, cit.

MARTÍNEZ i MARTÍNEZ, Ricard (coord.). *Derecho y cloud computing*, Civitas, Cizur, 2012

MARTÍNEZ i MARTÍNEZ, Ricard. *Seguridad, privacidad y confianza en la nube*, FIDE, 12 de diciembre de 2014, comentario de conferencia "Nuevo Standard de Seguridad y Privacidad en Cloud Computing: ISO 27018", FIDE, 18 de diciembre de 2014.

MARZO PORTERA, Ana "Privacidad y *cloud* computing, hacia dónde camina Europa", *Revista de Sociales y Jurídicas*, nº. 8, 2012, acceso en Dialnet, págs. 202-229, pág. 225.

MARZO PORTERA, Ana María y ORTEGA GIMÉNEZ, Alfonso. *Empresa y transferencia internacional de datos personales*, ICEX, Madrid, 2013

MELL, Peter y GRANCE Tim, *The NIST Definition of cloud Computing*, Version 15, October 7, 2009, http://csrc.nist.gov/groups/SNS/*cloud*-computing

MILLARD, Christopher (ed.). *Computing Law*, Queen Mary University of London, London, 2013.

MUÑOZ MACHADO, Santiago. *La regulación de la Red. Poder y Derecho en Internet,* Taurus, 2000.

PAQUETTE, S., JAEGER, P.T. y WILSON, S.C. "Identifying the security risks associated with governmental use of cloud computing". *Government Information Quarterly*. Volumen 27. 2010

PUYOL MONTERO, Javier. *Algunas consideraciones sobre cloud computing*, BOE-AEPD, Madrid, 2013. TÉLLEZ VALDÉS, Julio. *Lex cloud computing, Estudio Jurídico del Cómputo en la Nube de México*, UNAM, México, 2014, acceso completo en http://biblio.juridicas.unam.mx/libros/libro.htm?l=3249

REED, Chris. *Governance in cloud Computing*, *Queen Mary School of Law Legal Studies Research Paper* nº 157/2013, Acceso en SSRN y cloudlegalproject.org

RUBINSTEIN Ira, "Big Data: The End of Privacy or a New Beginning?", International Data Privacy Law (2013 Forthcoming), NYU School of Law, Public Law Research Paper No. 12-56. Acceso en SSRN.

SCHWARTZ, Paul M. "Information Privacy in the *cloud*" (mayo, 2013). *University of Pennsylvania Law Review,* Vol. 161, No. 1623 (2013), Acceso en SSRN.

SEMPERE SAMANIEGO, Javier, *Comentarios prácticos a la Propuesta de Reglamento de Protección de Datos de la Unión Europea*, 2014, acceso en www.privacidadlogica.es

SOLOVE, Daniel J. y HARTZOG, Woodrow, "The FTC and Privacy and Security Duties for the cloud" (April 14, 2014). 13 *BNA Privacy & Security Law Report* 577 (2014), acceso en SSRN.

TARRÉS VIVES, Marc. "Las normas técnicas en el Derecho Administrativo", en *Documentación administrativa*, nº 265-266, 2003 (Ejemplar dedicado a: Derecho administrativo, ciencia y tecnología), págs. 151-184.

TENE, Omer y POLONETSKY, Jules. "Judged by the Tin Man: Individual Rights in the Age of Big Data", en *Journal of Telecommunications and High Technology Law*, Forthcoming, 17 Aug 2013. Acceso en SSRN.

VALERO TORRIJOS, Julián. "La Administración Pública en la *nube*. Análisis de las implicaciones jurídicas desde la normativa sobre Administración electrónica", en MARTÍNEZ i MARTÍNEZ, Ricard (coord.), *Derecho y cloud computing*, cit.

VAN GYSEGHEM, Jean-Marc y otros. *Cloud computing and its implications on data protection*. Namur: CRID, 2010, http://www.crid.be/pdf/public/6471.pdf