Revista catalana de dret públic #51

www.rcdp.cat

ALGUNAS CUESTIONES CLAVE DE PROTECCIÓN DE DATOS EN LA NUBE. HACIA UNA «REGULACIÓN NEBULOSA»*

Lorenzo Cotino Hueso**

Resumen

Se abordan algunas deficiencias de la vieja y superada regulación nacional y europea de protección de datos aplicable a los servicios de la nube, así como acción de instituciones de protección de datos para corregirlas. También se analiza el esperado reglamento europeo de protección de datos, entre otros aspectos, su tendencia a reforzar las obligaciones del prestador de servicios de nube, como «encargado» de protección de datos. Igualmente se estudian las exigencias respecto del conjunto contractual y la subcontratación de servicios de nube. El uso de la nube frecuentemente supone una transferencia internacional de datos; al respecto se abordan vías de flexibilización de la necesidad de autorización previa (a través de las cláusulas contractuales tipo y *binding corporate rules*). Finalmente, se valora el papel de la normativa técnica privada sobre servicios de nube (como normas ISO o autorregulación del sector) y la futura normativa técnica que habrá de aprobar o la Comisión Europea o cada Estado, según se regule finalmente en el futuro reglamento europeo. Esta corregulación por normativa técnica pública o privada acaba conformándose como una regulación más o menos *nebulosa*.

Palabras clave: computación en la nube; nube; privacidad; protección de datos; seguridad de la información; derecho constitucional.

SOME KEY QUESTIONS REGARDING CLOUD DATA PROTECTION. TOWARDS A "NEBULOUS" REGULATION

Abstract

This article points out some of the deficiencies in the old, and now superseded, national and European data protection regulations applicable to cloud computing, and the action of data protection institutions to correct these deficiencies. It also analyses the awaited European data protection regulation on cloud services, in particular regarding the duties of the cloud service provider as "processor" and the cloud customer as "controller". Likewise, the article details demands regarding the contracts and outsourcing of cloud services. As regards the requirements for international transfers of data to third countries, the article looks at standard contractual clauses and Binding Corporate Rules as ways of relaxing the need for prior authorisation. Finally, the article discusses the role of private technical standards on cloud services (such as ISO standards or self-regulation rules), as well as the future technical regulations of public origin (by the European Commission or by each state, depending on the final version of the European data protection regulation). This co-regulatory complex implies, in the author's view, a "nebulous" legal system.

Key words: cloud computing; cloud; privacy; data protection; information security; Constitutional Law.

* El presente estudio se realiza en el marco de la estancia en la empresa Occentus Network S. L. (AEST/2015/023), así como del proyecto MINECO «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) y producto de investigación en el marco del proyecto «Gobierno abierto: participación, transparencia, datos abiertos, colaboración y gobierno en línea. Problemas y barreras jurídicas al desarrollo y gestión de la información pública» financiado por la Corporación Universitaria de Sabaneta, Unisabaneta, línea de «Derecho Público», Grupo de Investigación Pólemos, registro Colciencias COL0111291.

** Lorenzo Cotino Hueso, profesor titular, catedrático (acreditado) de Derecho Constitucional de la Universidad de Valencia y coordinador de la red <www.derechotics.com>; Departamento de Derecho Constitucional, Edificio departamental central, Avda. de los Naranjos, s/n, 46071 Valencia, <Lorenzo.Cotino@uv.es>, <www.cotino.es>.

Artículo recibido el 1.06.2015. Evaluación ciega: 25.06.2015 y 30.06.2015. Fecha de aceptación de la versión final: 17.09.2015.

Citación recomendada: Cotino Hueso, Lorenzo. «Algunas cuestiones clave de protección de datos en la nube. Hacia una "regulación nebulosa"». *Revista catalana de dret públic*, núm. 51 (diciembre 2015), pp. 85-103, DOI: 10.2436/20.8030.01.55.

CC BY NC ND

Sumario

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 de la nube, no es mucha la literatura jurídica española sobre la materia, aunque con estudios muy destacables.[1] Es algo mayor la atención en el ámbito europeo y anglosajón,[2] o de Estados Unidos.[3] Pese a que son diversas las cuestiones jurídicas que suscita la nube, por razones de espacio, el presente estudio focaliza el análisis en lo más vinculado a seguridad y protección de datos. Ello sin perjuicio de los particulares retos que suscita, entre otros, el uso de la nube por las Administraciones[4] o las crecientes facultades —y dificultades— de investigación de la nube y los deberes de colaboración de las empresas.[5]

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,[6] hacia la nube, la computación en la nube (*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,[7] estamos ante una

1 En español, sin perjuicio de las obras que se citan más adelante, una pionera atención merecen los trabajos de Leenes y Miralles en Martínez, David (coord.). *VI Congreso Internet, Derecho y Política. Cloud Computing: El Derecho y la Política suben a la Nube*. IDP. *Revista de Internet, Derecho y Política* [Barcelona: UOC], núm. 11 (2010). También disponible en línea aquí. Especialmente destaca la monografía coordinada por Martínez i Martínez, Ricard (coord.), *Derecho y cloud computing*. Cizur: Civitas, 2012; así como la monografía de Puyol Montero, Javier. *Algunas consideraciones sobre cloud computing*. Madrid: BOE-AEPD, 2013. En México, una descripción completa del tema en Téllez Valdés, Julio. *Lex cloud computing, Estudio Jurídico del Cómputo en la Nube de México*. México: UNAM, 2014. También disponible en línea aquí. De especial valor son los documentos institucionales de la AEPD (2013) y del Grupo de Trabajo del Artículo 29 (2012) que se citan más tarde. En la doctrina española cabe añadir estudios centrados mayormente en la cuestión de la transferencia internacional de datos, como los de Guasch y Soler, y de Marzo y Ortega. También hay aproximaciones más genéricas por Fernández Aller o Mexía.

2 Hay estudios iniciales, como Van Gyseghem, Jean-Marc y otros. *Cloud computing and its implications on data protection* [en línea]. Namur: CRID, 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 el 2014 se instituye el Microsoft Cloud Computing Centre (<www.mccrc.eu/>) del Queen Mary con la Universidad de Cambridge. Se puede acceder a casi todas las publicaciones jurídicas tanto en SSRN como en cloudlegalproject.org, aunque no a la monografía Millard, Christopher (ed.). *Computing Law*. Londres: Queen Mary University of London, 2013.

3 Sobre el régimen jurídico de la nube en Estados Unidos, Solove, Daniel J.; Hartzog, Woodrow. «The FTC and Privacy and Security Duties for the cloud» *13 BNA Privacy & Security Law Report* 577 (2014). También disponible en línea aquí. Y sobre disparidades y posibles choques entre normativa estadounidense y europea de protección de datos para la nube, Schwartz, Paul M. «Information Privacy in the Cloud». *University of Pennsylvania Law Review,* vol. 161, núm. 1623 (2013. También disponible en línea aquí.

4 La cuestión solo ha sido estudiada por 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*, ob. cit. También ver *Derecho, innovación y administración electrónica*. Sevilla: Derecho Global-Global Law Press, 2012. El autor remite a Paquette, S., Jaeger, P. T.; Wilson, S. C. «Identifying the security risks associated with governmental use of cloud computing». *Government Information Quarterly*, volumen 27 (2010). Aunque de mayor interés técnico que jurídico, Catteddu, D. *Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones*. ENISA, 2011.

5 Sobre el tema, «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 (acceso en <www.cotino.es>). Al respecto, hay que tener especialmente en cuenta la muy completa Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica; el proyecto se aprobó por el Gobierno el 13 de marzo de 2015 y, en un procedimiento de gran celeridad, por el Congreso el 19 de junio y definitivamente al momento de cerrar la última revisión de estas páginas. Esta nueva ley 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 mismo 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*.

6 Así, Grupo de Trabajo del artículo 29, *Dictamen 05/2012 sobre la computación en nube*. Dirección General de Justicia de la Comisión Europea, WP 196 01037/12/ES (julio 2012), p. 5. También disponible en línea aquí.

7 Así, Larry Ellison, CEO de Oracle en el 2009, diría que «Las nubes son vapor de agua. […] Esto no es más que un ordenador conectado a una red» en Venturebeat (accesible aquí). Y un importante analista de Gartner diría, el 8 de noviembre de 2010, que la

de las mayores revoluciones tecnológicas de los últimos tiempos. Y, como cualquier proceso evolutivo, el avance de la computación en la nube como paradigma tecnológico mundial representa un desafío en todos los órdenes.

La nube supone[8] 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 el 2005, para las corporaciones, las TIC dejan de ser una propiedad, para pasar a ser un servicio que adquieren como usuarios.[9] 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 localizada en cualquier lugar del mundo. El mismo prestador de servicios de nube puede, a su vez, variar constantemente la ubicación de 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 de la computación en la nube 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. Además 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 exclusiva 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 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; y 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 la nube, tanto públicas como privadas: infraestructura como servicio (*IaaS*, del ingés *infrastructure as a service*), nube de software como servicio (*SaaS*, del inglés *software as a service*), y plataforma como servicio (*PaaS*, del inglés *platform as a service*).

nube está en la cima de las «expectativas infladas». Así, en «Gartner Hype Cycle 2010: Cloud Computing at the Peak of Inflated Expectations», *Readwrite.com* (accessible aquí).

8 Para una aproximación general, y en especial las definiciones, se sigue: Mell, Peter; Grance, Tim. The NIST Definition of cloud Computing. Septiembre, 2011; Grupo de Trabajo del artículo 29, *Dictamen 05/2012*…, ob. cit., pp. 29 y ss.; ENISA *Cloud Computing: Benefits, risks and recommendations for information security* [en línea]; Agencia Española de Protección de Datos [AEPD]. *Guía para clientes que contraten servicios de cloud computing* [en línea] 2013. y *Orientaciones para prestadores de servicios de cloud computing* [en línea] 2013.

9 Carr, Nicholas. «The End of Corporate Computing». En: *MIT Sloan Management Review*, vol. 47, núm. 3 (abril 2005), pp. 67-73, p. 68. El autor lo es de la obra de referencia *The Big Switch: Rewiring the World, from Edison to Google*. Nueva York: W. W. Norton & Company, 2008.

La infraestructura 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 del tipo software como servicio (SaaS) el usuario cuenta con aplicaciones en la nube, como una aplicación de contabilidad, de correo electrónico, un *workflow*, 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 la 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 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 de la nube:[10]

- 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 lleva 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 este 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.

- 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. Las empresas, desde la más grande hasta 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 para acceder a distancia a la información de la empresa, con los peligros y fisuras de seguridad que ello puede generar.[11] Desde la perspectiva económica y como se recuerda desde Europa,[12] 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

10 Cloud Security Alliance [CSA]. *Guía para la seguridad en áreas críticas de atención en cloud computing*. Resumen ejecutivo. Versión 2 [noviembre 2009] del original *Security Guidance for Critical Areas of Focus in cloud computing V2*, CSA, 2009. [Trad. de ISMS Forum.]

11 Sobre el tema acaba de aparecer la monografía de Puyol Montero, Javier. *Una aproximación a la técnica «BYOD» y al control estratégico de las nuevas tecnologías en la empresa*. Valencia: Tirant lo Blanch, 2015.

12 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, p. 5. También disponible en línea aquí.

las inversiones en TIC). Un estudio para Microsoft[13] afirma que el la computación en la nube creará cerca de 14 millones de nuevos empleos en todo el mundo en el 2015; de ellos, 134 000 corresponderían a España.[14] En nuestro país hay algunas agrupaciones sectoriales, vinculadas al ámbito europeo.[15] Otros estudios afirman que se crearán hasta 800 000 empleos en Europa para el mismo periodo.[16] Los beneficios de la nube se estiman en 1,1 billones (europeos) de dólares.[17] Ello, y el ya comentado ahorro de costes y el aumento de la productividad que proporciona la computación en la nube, 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 europeas,[18] y especialmente en la española.[19] Es más, se tiene en cuenta que una mejora del marco jurídico de protección de datos puede contribuir al desarrollo del sector.[20]

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 la centralización de las aplicaciones y el almacenamiento de los datos origina una interdependencia de los proveedores de servicios.[21]

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 la infraestructura de los prestadores de servicios de nube, ya por los riesgos de seguridad en las continuas conexiones entre el usuario y el prestador.

13 Gantz, John F., Minton, Stephen; Toncheva, Anna. *Whitepaper. Cloud Computing's Role in Job Creation.* Framingham (EE. UU.), marzo de 2012, dato en la p. 2. También disponible en línea aquí.

14 Esta afirmación por Microsoft España aquí.

15 Así, en España la Agrupación Cloud Network o Euro Cloud España, 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, con 120 empresas y más de 800 profesionales asociados. También cabe tener en cuenta la Cloud Security Alliance, con ISMS en España tiene la iniciativa Cloud Security Alliance España (CSA-ES) que reúne a miembros representativos de la industria de la computación en la nube en España. Se trata de un foro de debate que promueve el uso de buenas prácticas para garantizar la seguridad y privacidad en el entorno de la computación en la nube y en el marco del cual se difunden estudios como el reciente ISMS-CSA-ES. *Estudio del Estado de la Seguridad en Cloud Computing* [en línea].

16 Roland Berger Strategy Consultant; SAP. *La supervivencia del más apto: Cómo puede Europa asumir un papel de liderazgo en la nube*, 2012. Ver, también <https://www.rolandberger.com/media/pdf/Roland_Berger_think_act_Cloud_Economy_20110922.pdf>.

17 Gantz, John F.; Minton, Stephen; Toncheva, Anna. *Whitepaper.* ... ob. cit., p. 2.

18 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. También disponible en línea aquí.

19 Agenda Digital para España, Ministerio de Industria, Energía y Turismo y por el Ministerio de Hacienda y Administraciones Públicas, febrero 2013. Entre los seis grandes objetivos y en el marco del desarrollo de la economía digital (el 2, p. 5), se propone «potenciar el desarrollo y uso del cloud computing» (p. 6). Asimismo, entre las propuestas para «Potenciar las industrias de futuro» (apdo. 2.6, pp. 28 y ss.) se considera la nube como «oportunidad industrial» y se formulan diversas propuestas concretas.

20 Así, *ibidem*, en concreto el punto 6, apdo. 4.3, p. 42.

21 Estos riesgos se siguen entre otros en *Wikipedia*, voz: «computación en la nube»: <http://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube>.

Los informes mundiales sobre seguridad en la nube[22] 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 el control de acceso a los recursos. El Grupo de Trabajo del artículo 29, por ejemplo, divide los riesgos, de un lado, en la falta de control de los datos, esto es: falta de disponibilidad, de portabilidad, de integridad, de confidencialidad de los datos, así como la complejidad y la dinámica de la cadena de subcontratación. De igual modo, la falta de aislamiento de datos de los distintos usuarios. Del otro lado se destaca el riesgo de la falta de transparencia: los usuarios no son conscientes de las amenazas y riesgos de los servicios, ni de la existencia de múltiples encargados del tratamiento y subcontratistas, así como de la ubicación de su información y si está fuera o dentro de la Unión Europea.[23]

La Cloud Security Alliance (CSA) señala como amenazas el abuso y mal uso de la computación en la nube (especialmente en servicios IaaS y PaaS —infraestructura y plataforma como servicio, respectivamente—); 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 accidentales. 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 destacan los riesgos por desconocimiento de con quién se comparte la infraestructura, así como que los intentos de acceso no autorizados pueden resultar muy importantes a la hora de decidir la estrategia de seguridad.[24] A los anteriores riesgos y problemas, Gartner añade otros riesgos de la nube, como es el teletrabajo y el acceso a datos fuera de las instalaciones de la empresa (BYOD) *supra* referidos; 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, porque en estos entornos puede ser una investigación casi imposible dado que 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 plazo, puesto que el mercado es cambiante y cabe la posibilidad de que el proveedor sea comprado o absorbido por alguno con mayores recursos.[25]

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 ponen en riesgo la disponibilidad de la información por parte del 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.[26]

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

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

23 Grupo de Trabajo del artículo 29. *Dictamen 05/2012*…, ob. cit., p. 6 y ss.

24 Estos riesgos son los reflejados por Cloud Security Alliance, *Top Threats to Cloud Computing V1.0* [en línea]. Marzo de 2010.

25 Gartner. *Assessing the Security Risks of Cloud Computing* [en línea]. Stamford, 2011.

26 INTECO-CERT, *Riesgos y amenazas en cloud computing* [en línea]. 2011, pp. 24 y ss.

información a otros), archivo a largo plazo y, por último, destrucción. Y, en la nube, los retos clave al respecto se centran en:[27] (1) la geolocalización de los datos —debe existir una garantía de que los datos estén donde legalmente sea posible—; (2) la eliminación efectiva y completa de los datos cuando se considere que son «destruidos»—debe existir una garantía de que los datos se eliminan adecuadamente—; (3) la diferenciación de los datos, especialmente los datos sensibles, respecto a los datos de otros clientes en su uso, almacenamiento o tránsito —debe existir una garantía de que los datos no se mezclan—; y (4) las 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 señalado Martínez,[28] 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,[29] sobre la que hoy hay bastante claridad. Pues bien, como ha recordado el Grupo de Trabajo del artículo 29[30] y la Agencia Española de Protección de Datos (AEPD),[31] el prestador de servicios de nube es, en términos del artículo 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.[32] No obstante, y como luego se aprecia, el marco contractual es clave para la definición de papeles y es prueba objetiva de 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 cuente 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 de Trabajo 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.[33]

27 Se sigue de Cloud Security Alliance (CSA), *Guía para la Seguridad*..., ob. cit., en concreto, 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, pp. 21 y ss.

28 Martínez i Martínez, Ricard. *Seguridad, privacidad y confianza en la nube*. FIDE (12 diciembre 2014), comentario de conferencia «Nuevo Standard de Seguridad y Privacidad en Cloud Computing: ISO 27018», FIDE, 18 diciembre 2014.

29 Así, dedica buena parte del mismo a esta cuestión Leenes, Ronald (2010). «¿Quién controla la nube?», ob. cit.

30 Grupo de Trabajo del artículo 29, *Dictamen 05/2012*…, ob. cit.

31 Tanto en Agencia Española de Protección de Datos [AEPD]. *Guía para clientes*…, ob. cit., como en Agencia Española de Protección de Datos [AEPD]. *Orientaciones para prestadores*…, ob. cit.

32 Agencia Española de Protección de Datos [AEPD]. *Orientaciones para prestadores*..., ob. cit.

33 Grupo de Trabajo del artículo 29. *Dictamen 05/2012*…, ob. cit.

2.2 Las cuestiones clave de protección de datos, la emergencia de un regulador nebuloso y las insuficiencias de la regulación actual

Como desde sus inicios puso en evidencia la Declaración de Independencia del Ciberespacio de 1996,[34] no son pocos los problemas que implica en general la regulación de internet. Se hace especialmente necesario un *derecho en red* con intervención más horizontal de todos los operadores; de igual modo, el derecho y las finalidades que con él pretenden los poderes públicos, para tener algún sentido, deben adecuarse en buena medida a un *código interno* que aúna el funcionamiento técnico y la realidad y usos de la red.[35] Aunque no es, en modo alguno, un fenómeno exclusivo de internet, en la red sí que se aprecia muy intensamente que hoy día la gobernación vertical y la heterorregulación por los poderes públicos queda en general obsoleta. La regulación que pretenda tener alguna eficacia debe ser el resultado de fórmulas de gobernanza en las que participe activamente el sector afectado sobre el que tienen que aplicarse las normas.[36] Pues bien, la regulación de la nube no es, en modo alguno, ajena a estos problemas. Fenómenos más recientes como el del *big data* evidencian, aún más si cabe, estos problemas y hacen inclinarse hacia formas de regulación suaves.[37] En el ámbito de la nube, Reed[38] ha insistido recientemente en modelos de corregulación trasnacional, en especial se insiste en que es necesario reforzar la legitimación de las normas. Y, frente a los esquemas clásicos de legitimación normativa, esto es, a partir de la heterorregulación del sector por parte del Estado, la legitimación que se reclama procede precisamente del propio sector afectado. Se afirma así que la regulación no debe venir únicamente de normas institucionales de poderes públicos, sino de la mano de un *regulador nebuloso* (*cloud-regulator*). Esta regulación nebulosa resulta de la que genera las normas con la participación de la comunidad afectada (instituciones, individuos y las entidades empresariales implicadas), y tal regulación tiene necesariamente que ser aceptada y hacerse propia por los Estados e instituciones, que tienen que hacer valer tales normas. Esta regulación nebulosa de la nube, como *infra* se concreta, parece que va *tomando cuerpo* en razón de la acción no normativa de autoridades de protección de datos, al mismo tiempo que la consolidación de regulación técnica de origen privado por parte del sector. Y sobre esta base ya preexistente van a aprobarse normas propiamente dichas por la Unión Europea, sus instituciones y los Estados. Estas normas contendrán disposiciones básicas más generales que, a su vez, reenviarán al desarrollo de futuras normativas técnicas. Y esta normativa más concreta que en su día se apruebe por instituciones europeas o por Estados, sin duda, tendrá bien en cuenta la normativa técnica privada preexistente.

Para asentar lo anterior, cabe tener en cuenta que, aunque no de manera exclusiva, el fenómeno de la nube atrae la cuestión de la protección de datos,[39] que es la que centra mayormente aquí el interés. Y en materia

34 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>)

35 Sobre la problemática de la regulación de la red, referencia obligada Lessig, Lawrence. *El código y otras leyes del ciberespacio.* Madrid: Taurus, 2001; y, en español, Muñoz Machado, Santiago. *La regulación de la Red. Poder y Derecho en Internet.* Madrid: Taurus, 2000. En general y más actual es la reflexión de Reed, Chris. *Making Laws for Cyberspace*. Oxford: Oxford University Press, 2012, capítulo 4.

36 Sobre gobernanza en general, puede seguirse mi estudio «El concepto "gobernanza" en la UE y su difícil aprehensión jurídica». En: García Herrera, Miguel Ángel. *Constitución y democracia: 25 años de Constitución democrática en España: (actas del congreso celebrado en Bilbao los días 19 a 21 de noviembre de 2003).* Vol. 2, 2005, pp. 283-304: También disponible en línea en: <www.cotino.es>).

37 En este ámbito de todo interés, Rubinstein subraya la necesidad de una «*big ethic data*» nutrida de heterorregulación, autorregulación y buenas prácticas de los agentes implicados: Rubinstein, Ira. «Big Data: The End of Privacy or a New Beginning?». International Data Privacy Law, *NYU School of Law, Public Law Research Paper*, núm. 12-56 (2012). También disponible en línea aquí. Tene, Omer; Polonetsky, Jules. «Judged by the Tin Man: Individual Rights in the Age of Big Data». *Journal of Telecommunications and High Technology Law*, 17 agosto 2013. También disponible en línea aquí. Estos autores son escépticos de una heterroregulación «fuerte», pero sí señalan la necesidad de directrices y regulaciones legales y técnicas.

38 Reed, Chris. «Governance in Cloud Computing». *Queen Mary School of Law Legal Studies Research*, núm. 157 (2013). También disponible en línea aquí.

39 Además de los estudios en los que se aborda de modo más concreto, un análisis general de la cuestión se encuentra en 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*, núm. 10 (2012), pp. 125-145. También disponible en línea aquí. También, una aproximación general en García Mexía, Pablo. «Cloud computing: sus implicaciones legales». *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 23 (2010), pp. 79-88. De este autor, accesible en la red, *Cloud Computing. Sus dilemas legales.*

de protección de datos, la ley aplicable es la del lugar del cliente de servicios de la nube,[40] 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).[41]

Miralles[42] ha sintetizado los aspectos más relevantes del nexo de la protección de datos y la computación en la nube: 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 en la nube 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 europea de protección de datos para la nube.[43] Como especialmente recuerda Marzo, la Directiva 95/46/CE está muy desfasada y se ha convertido en una traba para las relaciones entre Europa y los terceros países. Y, como luego se concreta, el Grupo de Trabajo del Artículo 29 y la AEPD han sido proactivos en los últimos años para, a través de dictámenes, guías, orientaciones, cláusulas contractuales generales, etc., colmar las lagunas e incertidumbres de una normativa no concebida para la nube. Este *soft law* ha pasado a ser el marco de certidumbre en el sector a la espera de una normativa que no acaba de llegar. En todo caso, dado que las empresas y Administraciones públicas españolas no pueden abandonar el barco del «progreso tecnológico»,[44] necesariamente tienen que arriesgarse a contratar servicios de computación en la nube 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 computación en la nube 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

Como es sabido, desde enero del 2012 se maneja el texto de un futuro Reglamento europeo de protección de datos, del que hay diversas versiones: de la Comisión (2012),[45] del Parlamento (marzo del 2014),[46] y del Consejo (junio del 2015)[47] y parece ser que se aprobará en el 2016. Aunque lamentablemente no hay referencia expresa a los servicios de la nube, obviamente la regulación proyectada se proyecta para la computación en la nube.[48] Entre otros aspectos, el Reglamento destaca por la figura del delegado de protección de datos

40 Así, en especial Grupo de Trabajo del artículo 29, *Dictamen 05/2012*…, ob. cit., p. 8 y *Dictamen 8/2010 sobre la ley aplicable*.

41 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.

42 Martín Miralles, Ramón. «Cloud computing y protección de datos». En: Martínez, David (coord.). *VI Congreso Internet, Derecho y Política. Cloud Computing*..., ob. cit.

43 Un análisis concreto sobre disparidades y posibles choques entre normativa americana y europea de protección de datos para la nube, Schwartz, Paul M. «Information Privacy in the Cloud». *University of Pennsylvania Law Review*, vol. 161, núm. 1623 (2013). También disponible en línea aquí.

44 Marzo Portera, Ana. «Privacidad y cloud computing, hacia dónde camina Europa». *Revista de Sociales y Jurídicas*, núm. 8 (2012), pp. 202-229, p. 225. También disponible en línea aquí.

45 Propuesta de Reglamento por la Comisión Europea, de 25 de enero de 2012, COM(2012) 11 final.

46 Texto 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.*

47 Texto versión de 11 de junio de 2015 del Consejo de la Unión Europea, Doc. 9565/15.

48 El análisis más extenso a este respecto, con recomendaciones para el legislador europeo, se debe a Hon, W. Kuan [*et al.*]. «Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation». *Queen Mary School of Law Legal Studies*

(*DPO*, del inglés *data protection officer*, arts. 35-37). Dicha persona —en nuestro caso, 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 generar todas unas buenas prácticas y transparencia 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:[49] «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».[50] Y, además de la regulación ya contenida en el futuro artículo 23, puede pensarse que esta 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. 2.º y 3.º y art. 86). Podría así esperarse que, en unos años, diversos servicios de la nube pasen a ser un sector bastante regulado de manera concreta y homogénea y para toda la Unión Europea por la Comisión. Todo ello, sin perjuicio de que dicha regulación quizá llegue tarde pare remover usos, prácticas y autorregulación ya consolidados en el sector. También y para estimular el cumplimiento, se prevé que estas exigencias de privacidad por defecto y en el diseño pasen a ser «un requisito previo para las licitaciones de contratos públicos» (art. 23. 1 bis, versión Parlamento 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, puesto que los cambios parecen muy sustanciales. No en vano, en junio del 2015 se conoció la versión del Reglamento del Consejo de la Unión Europea.[51] Por lo que ahora interesa, se refuerza mucho el papel de los Estados miembros, puesto que se elimina toda remisión o delegación de atribuciones a la Comisión para hacer el papel de regulador técnico homogéneo. En esta versión, se quita muchísimo poder a la Comisión y se deja la futura regulación técnica en manos de cada uno de los 28 Estados miembros. De así ser, se incrementa el riesgo de falta de regulación y, sobre todo, de falta de homogeneidad de la regulación técnica. De seguirse esta vía, la regulación de la nube puede hacerse mucho más nebulosa si cabe.

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 servicios de nube

Según se ha señalado, el cliente de servicios de la nube es «responsable» de la 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 AEPD ha adoptado un papel activo para difundir el conocimiento de esta responsabilidad y de los

Research, núm. 172 (2014). También disponible en línea aquí. Y desde la misma institución se acaba de publicar Hon, W. Kuan [*et al.*]. «Policy, Legal and Regulatory Implications of a Europe-Only Cloud». *Queen Mary School of Law Legal Studies Research*, núm. 191 (2015). También disponible en línea aquí. En español, sobre el futuro reglamento hay un amplio comentario, de 500 pp., de Sempere Samaniego, Javier. *Comentarios prácticos a la Propuesta de Reglamento de Protección de Datos de la Unión Europea*, [en línea]. 2014.

49 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/>.

50 Considerando 61 en la versión de marzo de 2014 del Parlamento Europeo, ob. cit.

51 Se trata del texto de 11 de junio de 2015 (OR. en) 9565/15 (expte: 2012/0011 [COD]).

elementos de juicio para tomar decisiones.[52] Así, por ejemplo, ha señalado las preguntas que debe formularse la empresa o Administración (a través del futuro delegado de protección de datos) antes de contratar servicios de nube:

> 1.-¿Qué debo analizar y tener en cuenta antes de contratar servicios de 'cloud computing'?; 2.- Desde la perspectiva de la normativa de protección de datos, ¿cuál es mi papel como cliente de un servicio de 'cloud'?; 3.- ¿Cuál es la legislación aplicable?; 4.- ¿Cuáles son mis obligaciones como cliente?; 5.- ¿Dónde pueden estar ubicados los datos personales? ¿Es relevante su ubicación?; 6.- ¿Qué garantías se consideran adecuadas para las transferencias internacionales de datos?; 7.- ¿Qué medidas de seguridad son exigibles?; 8.- ¿Cómo puedo garantizar o asegurarme de que se cumplen las medidas de seguridad?; 9.- ¿Qué compromisos de confidencialidad de los datos personales debo exigir?; 10.- ¿Cómo garantizo que puedo recuperar los datos personales de los que soy responsable (portabilidad)? 11. ¿Cómo puedo asegurarme de que el proveedor de cloud no conserva los datos personales si se extingue el contrato? ; 12.- ¿Cómo puedo garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO)?

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»[53] (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 de 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.[54]

Como señala el Grupo de Trabajo del Artículo 29 de la UE,[55] respecto del futuro Reglamento europeo, la empresa de servicios de nube (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,[56] hay que sumar tradicionales exigencias a un encargado que aloja datos.[57] Y cabe 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. 12.2 y 3 LOPD y art. 22 RLOPD). En la versión inicial del Reglamento europeo de la Comisión, en su artículo 18 se incluyó un novedoso «derecho a la portabilidad», que desaparece en la versión del Parlamento, del 2014, y reaparece en la versión del Consejo, de 2015 (art. 18). 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).[58] En este sentido cabe recordar que el artículo 81.8 RLOPD permite aplicar diferentes niveles de

52 Agencia Española de Protección de Datos [AEPD]. *Guía para clientes que contraten servicios de cloud computing* [en línea] 2013.

53 Agencia Española de Protección de Datos [AEPD]. *Orientaciones para prestadores*..., ob. cit.

54 Grupo de Trabajo del artículo 29. *Dictamen 05/2012*…, ob. cit. Ver apartado 3.4.1.1 p. 18.

55 Grupo de Trabajo del artículo 29. *Dictamen 05/2012*…, ob. cit., pp. 26 y ss.

56 Cabe destacar el reciente estudio AA. VV. *La responsabilidad legal de las empresas frente a un ciberataque*, ISMS Forum, ENATIC, Abogacía Española, Inteco, 2014. También disponible en línea aquí. Ahí se analiza la responsabilidad de la empresa atacada, ya como cliente, ya como proveedora de servicios de las responsabilidades.

57 En particular recogidas en el Informe 574/2009 de la AEPD sobre el carácter de encargado del tratamiento de un prestador de servicios de alojamiento (acceso en web AEPD).

58 *Ibidem*, en el mismo sentido Informe 620/2009.

seguridad a un fichero. Asimismo, el encargado del tratamiento debe elaborar el correspondiente documento de seguridad (art. 82. 2 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 servicios de nube: 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 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 a que haya accedido el cliente. Todo este conjunto contractual juega un papel clave en los servicios de la nube como garantía no solo 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;[59] 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 21.2 RLOPD) exige mayores garantías, como ha ratificado la STS de 15 de julio de 2010, FJ 10.[60] Así, las garantías deben darlas los socios de prestadores de nube —en cualquiera de las figuras de *reseller*, agregadores de servicios de nube, *cloud builders*, proveedores de aplicaciones, etc.—, y los que proporcionan servicios contratando directamente con los clientes.

El Grupo de Trabajo del artículo 29 ha recordado diversos contenidos y garantías en el contrato de servicios de nube,[61] los mismos tienen su reflejo en la guía de la AEPD para los clientes de servicios.[62] Y hay que buscar un cuerpo contractual equilibrado entre las responsabilidades de cliente (responsable del tratamiento) y empresa de nube (encargada del tratamiento).[63]

59 Entre otros, dedica alguna atención a las subcontrataciones Fernández-Aller, Celia. «Algunos retos…», ob. cit., pp. 137-138.

60 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 Agencia Española de Protección de Datos [AEPD]. *Guía para clientes…*, ob. cit., como en Agencia Española de Protección de Datos [AEPD]. *Orientaciones para prestadores…*, ob. 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».

61 Grupo de Trabajo del artículo 29. *Dictamen 05/2012*…, ob. cit., pp. 9 y ss. y 14 y ss.

62 Agencia Española de Protección de Datos [AEPD]. *Guía para clientes…*, ob. cit.

63 Un análisis de los contratos, Bradshaw, Simon; Millard, Christopher; Walden, Ian. «Contracts for clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services». *Queen Mary School of Law Legal Studies Research*, núm. 63 (2010). También disponible en línea aquí.

Entre estos contenidos y garantías 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 que tiene el proveedor de nombrar a todos los subcontratistas contratados.[64] 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.[65] Asimismo ha de tener garantías efectivas frente a una posible infracción del contrato por el proveedor.[66]

El contrato debe determinar medidas de seguridad técnica y de organización (en virtud del artículo 17, apartado 2, de la Directiva). De igual modo,[67] 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 datos, en consonancia con los requisitos correspondientes y con sujeción a las medidas más estrictas previstas en la legislación nacional de los clientes. Habrá que indicarse que solo 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 este, 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.[68]

No hay que olvidar que no solo están en juego los derechos e intereses de las partes, sino la garantía de un derecho fundamental de muchos sujetos 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 servicios de nube contratadas y subcontratadas: cláusulas contractuales tipo y normas corporativas vinculantes

Casi por defecto, el uso de la nube implica el trasiego internacional de datos,[69] bien porque el prestador de servicios esté en el extranjero, bien porque, como se ha indicado, lo natural en la nube es la subcontratación

64 Grupo de Trabajo del artículo 29. *Dictamen 05/2012*…, ob. cit., pp. 9 y ss. Como se ha señalado, obligación confirmada por la STS de 15 de julio de 2010, FJ 10º.

65 *Ibidem*, pp. 23 y ss.

66 *Ibidem* punto 3.3.2 p. 11.

67 *Ibidem*. 23 y ss.

68 *Ibidem*, p. 16.

69 Sobre el tema, cabe seguir Agencia Española de Protección de Datos [AEPD]. *Transferencias Internacionales de datos para la realización de un tratamiento por cuenta del responsable del fichero. Informe 2001-0000* [en línea]. En la doctrina en general, Marzo Portera, Ana María; Ortega Giménez, Alfonso. *Empresa y transferencia internacional de datos personales*. Madrid: ICEX, 2013; y los autores de dos tesis doctorales sobre el tema: por un lado, Guasch Portas, Vicente. —«La transferencia internacional de datos de carácter personal». RDUNED. *Revista de derecho UNED*, núm. 11 (2012), pp. 413-454. También disponible en línea aquí; y, por otro, la premiada tesis doctoral Ortega Giménez, Alfonso. *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, septiembre de 2014 (publicada en la web de la AEPD).

de servicios por los prestadores de servicios. El marco normativo y las instituciones deben adaptarse a esta realidad y, al mismo tiempo, garantizar la seguridad, privacidad y el cumplimiento de la legalidad, permitiendo tales las transferencias internacionales de datos. Y deben permitirse las mismas asegurando 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 los datos o el prestador estén en países terceros que no cuenten con un nivel adecuado de protección de datos (Suiza, Canadá, Argentina, isla de Guernsey, isla de Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda y ciertas compañías estadounidenses).[70] En tales casos, por principio es requisito una autorización del director de la AEPD 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 26.2 de la Directiva 95/46/CE de protección de datos).[71] 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, este debe estipular de modo concreto cómo el prestador de servicios ha de aplicar los principios de la protección de datos y, al mismo tiempo, 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 el año 2012 un nuevo conjunto de cláusulas contractuales para facilitar la subcontratación que ha de preverse en el contrato.[72] 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 previa de la autoridad de protección de datos competente. La ventaja para las empresas de servicios de nube 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. Solo tendrán que notificar —no pedir autorización— cada nueva transferencia internacional para que esta quede registrada.[73]

70 Respecto de estos países hay decisiones de la Comisión Europea desde el 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.
- 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 EE. UU., 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 aquí.

71 Sobre el tema, los trabajos ya referidos de Giménez y Marzo, y el de Guasch Portas, Vicente; Soler Fuensanta, José Ramón. «Cloud computing, cláusulas contractuales y reglas corporativas vinculantes». RDUNED. *Revista de Derecho UNED*, núm. 14 (2014), pp. 247-269. También disponible en línea aquí. También García del Poyo Vizcaya, Rafael. «La contratación empresarial de servicios de cloud computing». En: Martínez i Martínez, Ricard. *Derecho y cloud computing*. Cizur: Civitas, 2012, pp. 179-200, en especial, 186 y ss.

72 Las mismas fueron 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 de septiembre de 2012. El contenido es similar al de las clausulas tipo de la Comisión.

73 Entre otros, lo explican Guasch Portas, Vicente; Soler Fuensanta, José Ramón. «Cloud computing…», ob. cit. pp. 263 y ss.

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.[74] 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 Para concluir, hacia la «regulación nebulosa». La normativa y estándares técnicos a cumplir por el prestador de la nube, especial referencia a la nueva ISO/IEC 27018:2014 de 27 de julio de 2014

La complejidad de la cuestión, de los sujetos intervinientes, la necesidad práctica de confianza y seguridad por las partes y, en especial, la responsabilidad que adquiere el cliente de nube y la ponderación de riesgos que debe realizar, inclinan hacia la adopción de estándares técnicos por los prestadores de nube.

Como se ha dicho, el cliente es responsable de la elección del proveedor y del servicio, con todas las consecuencias jurídicas que pueden derivarse; debe acceder a la información que la empresa de nube le facilite; y, al fin y al cabo, controlarlo y auditarlo. Es por ello que el esquema se hace mucho más sencillo merced a las certificaciones del cumplimiento de normas técnicas por el prestador de servicios. 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 reciente ISO/IEC 27018:2014 de 27 de julio de 2014[75] de seguridad en la nube.

El sector de prestación de servicios de la nube necesariamente va a tender al seguimiento de la misma, pues incorpora la experiencia de las normas ISO 27000 adecuadas para los servicios de nube, y la norma ISO/IEC 27018:2014 tiene muy presente la normativa europea y el inminente reglamento europeo de protección de datos. El cumplimiento de esta norma implica y exige el cumplimiento de la legalidad aplicable. Como recientemente recuerda Martínez, aspectos como la privacidad por defecto (*data minimization* y *collection limitation*), la definición de aspectos como la conservación de datos, la *accountability* y la previsión de aspectos como la notificación de violaciones de seguridad o de la intervención de poderes del Estado requiriendo datos, constituyen elementos cruciales.[76] Esta norma técnica establece los objetivos de control y directrices para medidas de protección de información de identificación personal (PII, del inglés *personally identifiable information*), de conformidad con los principios de privacidad. En particular, la norma ISO/IEC 27018: 2014 especifica las directrices basadas en la norma ISO/IEC 27002, teniendo en cuenta los requisitos normativos para la protección de información de identificación personal. Esta nueva norma técnica de calidad es aplicable a todos los tipos y tamaños de organizaciones, incluidas las empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, que proporcionan servicios de procesamiento de información como procesadores de PII a través de la computación en la nube bajo contrato con otras organizaciones.

Habrá que estar pendiente de las posibilidades reales de implantación y cumplimiento de esta nueva norma técnica en el sector, por cuanto puede ser un instrumento muy efectivo tanto para el cliente y la empresa, como para la garantía y seguridad de los datos e información de los ciudadanos. De igual modo, habrá que tener en cuenta el difícil ensamblaje entre la normativa técnica y la heterorregulación pública por parte de la Unión Europea, la Comisión Europea o los Estados miembros. Así se ha expuesto *supra* en el apartado 2.2 y se está a la espera de que el Reglamento definitivo especifique quién será responsable de la concreción normativa y técnica, la Comisión o cada Estado miembro.

74 Al respecto, ver Grupo de Trabajo del artículo 29. *Dictamen 05/2012*…, ob. cit., p. 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.

75 «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». En español, sobre esta nueva norma técnica, una descripción aquí.

76 Martínez i Martínez, Ricard. *Seguridad, privacidad y confianza en la nube*…, ob. cit.

Como es sabido, es bien problemática la integración de las normas técnicas en el ordenamiento jurídico, entre otros motivos porque muchas veces son normas que no son públicas, sino que están protegidas por la propiedad intelectual. Las vías de integración de las normas técnicas privadas en la norma jurídica pública es variada: a través de reenvíos desde la normativa pública a la privada o remisiones directas o indirectas a las distintas versiones que se vayan produciendo de la norma técnica privada,[77] para asegurar así la adecuación sin necesidad de modificación normativa y delegando grandes espacios a lo privado. Como se dijo (*supra* 2.2), la normativa técnica pública quedará más en manos de la Comisión Europea o más en el ámbito normativo estatal interno. Y es pensable que la futura normativa técnica que apruebe la Comisión o cada Estado miembro siga de más cerca o de más lejos y tenga gran conexión con la normativa técnica privada que se va desarrollando para el ámbito de la nube. La voluntad del Consejo de la Unión Europea de junio del 2015 prácticamente anula el futuro desarrollo técnico normativo por la Comisión. Si finalmente se impone esta voluntad más estatalista, no es nada descartable que muchos Estados miembros que deberían regular aspectos técnicos y concretos de la nube, simplemente, no lo hagan. En este supuesto de vacío e indefinición normativa, el protagonismo de la normativa técnica privada puede ser si cabe, mayor.

Como se ha señalado, muy posiblemente cuando se desarrolle esta normativa técnica por la Comisión o cada Estado, 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 corregulación trasnacional del sector con ciertas garantías de exigibilidad y cumplimiento.

Bibliografía

AA. VV. *La responsabilidad legal de las empresas frente a un ciberataque*. ISMS Forum, ENATIC, Abogacía Española, Inteco, 2014. También disponible en línea aquí.

Agencia Española de Protección de Datos [AEPD]. *Transferencias Internacionales de datos para la realización de un tratamiento por cuenta del responsable del fichero. Informe 2001-0000* [en línea].

—*Guía para clientes que contraten servicios de cloud computing* [en línea].

—*Orientaciones para prestadores de servicios de cloud computing* [en línea] 2013.

—*Informe 0574/2009* (sobre el carácter de encargado del tratamiento de un prestador de servicios de alojamiento [en línea].

Bradshaw, Simon; Millard, Christopher; Walden, Ian. «Contracts for clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services». *Queen Mary School of Law Legal Studies Research*, núm. 63 (2010). También disponible en línea aquí.

Carr, Nicholas. «The End of Corporate Computing». *MIT Sloan Management Review,* vol. 47, núm. 3 (abril 2005), pp. 67-73. También disponible en línea aquí.

Carr, Nicholas. *The Big Switch: Rewiring the World, from Edison to Google. Nueva York: W. W. Norton & Company*, 2008.

Catteddu, D. *Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones* [en línea]. ENISA, 2011.

Cloud Security Alliance [CSA]. *Guía para la seguridad en áreas críticas de atención en cloud computing*. Resumen ejecutivo. Versión 2 [noviembre 2009] del original *Security Guidance for Critical Areas of Focus in cloud Computing V2*, CSA, 2009. [Trad. de ISMS Forum.]

—*Top Threats to cloud Computing V1.0* [en línea], marzo de 2010.

77 Sobre este interesante tema, por todos, Tarrés Vives, Marc. «Las normas técnicas en el Derecho Administrativo». *Documentación administrativa*, núm. 265-266 (2003) (ejemplar dedicado a: derecho administrativo, ciencia y tecnología), pp. 151-184, en concreto, ver pp. 170 y ss. (Tarrés es autor también de monografía sobre el tema). De modo más indirecto, es referencia Darnaculleta, María M. *Autorregulación y Derecho Público: la autorregulación regulada*. Barcelona: Marcial Pons, 2005.

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. También disponible en línea aquí.

ENISA. *Cloud Computing: Benefits, risks and recommendations for information security* [en línea].

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*, núm. 10 (2012), pp. 125-145. También disponible en línea aquí.

Gantz, John F., Minton, Stephen; Toncheva, Anna. *Whitepaper. Cloud Computing's Role in Job Creation.* Framingham (EE. UU.), marzo de 2012. También disponible en línea aquí.

García del Poyo Vizcaya, Rafael. «La contratación empresarial de servicios de cloud computing». En: Martínez i Martínez, Ricard. *Derecho y cloud computing*. Cizur: Civitas, 2012, pp. 179-200, en especial, 186 y ss.

García Mexía, Pablo. «Cloud computing: sus implicaciones legales». *Revista Aranzadi de derecho y nuevas tecnologías*, núm. 23 (2010), pp. 79-88.

García Mexía, Pablo. *Cloud Computing. Sus dilemas legales* [en línea].

Gartner. *Assessing the Security Risks of Cloud Computing* [en línea]. Stamford, 2011.

Grupo de Trabajo del Artículo 29. *Dictamen 05/2012 sobre la computación en nube*. Dirección General de Justicia de la Comisión Europea, WP 196 01037/12/ES (julio 2012), p. 5. También disponible en línea aquí.

—*Dictamen 8/2010 sobre la ley aplicable.* Dirección General de Justicia de la Comisión Europea, WP 179 0836-02/10/ES (diciembre 2010). También disponible en línea aquí.

Guasch Portas, Vicente; Soler Fuensanta, José Ramón. «Cloud computing, cláusulas contractuales y reglas corporativas vinculantes». RDUNED. *Revista de Derecho UNED*, núm. 14 (2014), pp. 247-269. También disponible en línea aquí.

—«La transferencia internacional de datos de carácter personal». RDUNED. *Revista de derecho UNED*, núm. 11 (2012), pp. 413-454. También disponible en línea aquí.

Hon, W. Kuan [*et al.*]. «Cloud Accountability: The Likely Impact of the Proposed EU Data Protection Regulation». *Queen Mary School of Law Legal Studies Research*, núm. 172 (2014). También disponible en línea aquí.

—«Policy, Legal and Regulatory Implications of a Europe-Only Cloud». *Queen Mary School of Law Legal Studies Research*, núm. 191 (2015). También disponible en línea aquí.

INTECO-CERT. *Riesgos y amenazas en cloud computing* [en línea]. 2011.

ISMS-CSA-ES. *Estudio del Estado de la Seguridad en Cloud Computing* [en línea].

Leenes, Ronald. «¿Quién controla la nube?». En: Martínez, David (coord.). *VI Congreso Internet, Derecho y Política. Cloud Computing: El Derecho y la Política suben a la Nube*. IDP. *Revista de Internet, Derecho y Política* [Barcelona: UOC], núm. 11 (2010). También disponible en línea aquí.

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

Martín Miralles, Ramón. «Cloud computing y protección de datos». En: Martínez, David (coord.). Monográfico "VI Congreso Internet, Derecho y Política. Cloud Computing: El Derecho y la Política suben a la Nube". IDP. *Revista de Internet, Derecho y Política* [Barcelona: UOC], núm. 11 (2010). También disponible en línea aquí.

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

—*Seguridad, privacidad y confianza en la nube*. FIDE (12 diciembre 2014) [comentario de conferencia].

—«Nuevo Standard de Seguridad y Privacidad en Cloud Computing: ISO 27018», FIDE, 18 diciembre 2014.

Marzo Portera, Ana María. «Privacidad y cloud computing, hacia dónde camina Europa». *Revista de Sociales y Jurídicas*, núm. 8 (2012), pp. 202-229 También disponible en línea aquí.

Marzo Portera, Ana María; Ortega Giménez, Alfonso. *Empresa y transferencia internacional de datos personales*. Madrid: ICEX, 2013.

Mell, Peter; Grance, Tim. The NIST Definition of cloud Computing [en línea]. Version septiembre 2011.

Millard, Christopher (ed.). *Computing Law*. Londres: Queen Mary University of London, 2013.

Ministerio de Industria, Energía y Turismo y Ministerio de Hacienda y Administraciones Públicas. *Agenda Digital para España* [en línea] febrero 2013.

Muñoz Machado, Santiago. *La regulación de la Red. Poder y Derecho en Internet.* Madrid: Taurus, 2000.

Paquette, S.; Jaeger, P. T.; 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*, Madrid: BOE-AEPD, 2013.

Reed, Chris. «Governance in Cloud Computing». *Queen Mary School of Law Legal Studies Research*, núm. 157 (2013). También disponible en línea aquí.

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

Rubinstein, Ira. «Big Data: The End of Privacy or a New Beginning?». International Data Privacy Law, *NYU School of Law, Public Law Research Paper*, núm. 12-56 (2012). También disponible en línea aquí.

Schwartz, Paul M. «Information Privacy in the Cloud». *University of Pennsylvania Law Review*, vol. 161, núm. 1623 (2013). También disponible en línea aquí.

Sempere Samaniego, Javier. *Comentarios prácticos a la Propuesta de Reglamento de Protección de Datos de la Unión Europea* [en línea]. 2014.

Solove, Daniel J.; Hartzog, Woodrow. «The FTC and Privacy and Security Duties for the cloud» *13 BNA Privacy & Security Law Report* 577 (2014). También disponible en línea aquí.

Tarrés Vives, Marc. «Las normas técnicas en el Derecho Administrativo». *Documentación administrativa*, núm. 265-266 (2003) (ejemplar dedicado a: derecho administrativo, ciencia y tecnología), pp. 151-184.

Tene, Omer; Polonetsky, Jules. «Judged by the Tin Man: Individual Rights in the Age of Big Data». *Journal of Telecommunications and High Technology Law*, 17 agosto 2013. También disponible en línea aquí.

Téllez Valdés, Julio. *Lex cloud computing, Estudio Jurídico del Cómputo en la Nube de México*. México: UNAM, 2014. También disponible en línea aquí.

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*. Cizur: Civitas, 2012.

Van Gyseghem, Jean-Marc [*et al.*]. *Cloud computing and its implications on data protection* [en línea]. Namur: CRID, 2010.