PRIVACIDAD Y CLOUD COMPUTING, HACIA DÓNDE CAMINA EUROPA

Ana María Marzo Portera

Abogado Ilustre Colegio de Abogados de Madrid

Sumario: ***I.- Introducción .II.- Sobre la revisión de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. III.- La opinión del Grupo de Trabajo del artículo 29 y la Agencia Española de Protección de Datos. IV.- Situación actual del cloud computing en el marco de las normas europeas. V.- Situación actual del cloud computing en el marco de nuestro derecho interno. VI.- Conclusiones e impactos. VII.- Bibliografía y documentación consultada.***

Enviado: 01/11/2011

Aceptado: 02/11/2011

PRIVACIDAD Y CLOUD COMPUTING, HACIA DÓNDE CAMINA EUROPA[1]

Sumario: ***I.- Introducción .II.- Sobre la revisión de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. III.- La opinión del Grupo de Trabajo del artículo 29 y la Agencia Española de Protección de Datos. IV.- Situación actual del cloud computing en el marco de las normas europeas. V.- Situación actual del cloud computing en el marco de nuestro derecho interno. VI.- Conclusiones e impactos. VII.-Bibliografía y documentación consultada.***

Resumen:

El objeto de la ponencia es analizar los requisitos que Europa establece a través de su normativa para permitir la realización de transferencias internacionales de datos a terceros países en un modelo de negocio en auge como es el cloud computing. Analizar si dichos requisitos son flexibles o si por el contrario su taxatividad y rigidez está impidiendo que las empresas europeas puedan cumplirlos. En este marco la pregunta es si las empresas europeas están cumpliendo la Directiva a la hora de contratar el cloud computing a prestadores de servicios ubicados en terceros países y si en caso negativo, ello pone en riesgo la seguridad de los datos personales que los prestadores de servicio almacenan. En la ponencia se analizará si Europa debería replantearse la necesidad de flexibilizar los requerimientos legales para la realización de transferencias internacionales de datos en modelos como el cloud computing, manteniendo en todo caso, las garantías y los derechos de los ciudadanos.

[1] (Basado en la ponencia elaborada por la misma autora seleccionada para el taller 11 "privacidad en la nube" en el Encuentro Internacional de Seguridad de la Información -ENISE-2011 organizado por INTECO).

Palabras clave: Seguridad jurídica, seguridad técnica y organizativa, contrato de acceso a datos, Cloud computing, datos de carácter personal, privacidad, responsabilidad, transferencias internacionales de datos.

I. Introducción.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante 95/46/CE) consagró dos de las ambiciones más antiguas del proyecto de integración europea: la realización del mercado interior logrando la libre circulación de datos personales y la protección de los derechos y libertades fundamentales de las personas.

Lo que quizás aún no era predecible es la amplísima repercusión que tendría esta Directiva en un futuro no muy lejano y las diversas consecuencias que traería consigo respecto de los nuevos modelos económicos y sociales. A ello ha contribuido no obstante el hecho de que Internet se ha convertido en un vehículo universal y global donde se han desarrollado y han encontrado soporte no solo los modelos de negocio del sector privado sino también la prestación de servicios públicos al ciudadano y las actividades y prácticas de ocio en el ámbito doméstico.

Si en el marco europeo, la diversidad de enfoques nacionales y la ausencia de un sistema de protección de la intimidad a escala comunitaria constituyeron un obstáculo a la realización del mercado interior que motivó la aprobación de la Directiva 95/46/CE, años después esta misma Directiva es la que está entorpeciendo el intercambio transfronterizo de datos con otros países del entorno extracomunitario.

Así, aunque en respuesta a la evolución tecnológica otras Directivas europeas convirtieron los principios expuestos en la Directiva 95/46/CE en normas específicas para el sector de las telecomunicaciones, el resultado no ha cambiado, en la actualidad

siguen sin resolverse algunos problemas derivados de las transferencias de datos personales a los denominados "terceros países"[2].

En realidad, a pesar de que mediante la Directiva 2002/58/CE relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas, de 12 de julio de 2002 y la más reciente Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 por la que se modifica la anterior, se ha adaptado la normativa a la evolución de los mercados y tecnologías de servicios de comunicación electrónica con el fin de ofrecer el mismo nivel de protección de los datos personales y la intimidad para todas las tecnologías utilizadas, Europa sigue enfrentada a los mercados en Estados Unidos y otros terceros países, en clara desventaja comercial y económica, respecto de la explotación comercial de determinados modelos de negocio, de la implantación de nuevas técnicas de marketing en línea y en definitiva respecto de los tratamientos a que pueden ser sometidos los datos personales de los ciudadanos y usuarios de los servicios que la industria ofrece a través de Internet.

A ello hay que añadir que la evolución de la tecnología de la información y la creciente preocupación por la seguridad, han avivado el debate sobre la protección de datos en el marco social. Desde la aprobación de la Directiva 95/46/CE, se ha producido un aumento exponencial del número de hogares, empresas y administraciones públicas conectadas a Internet, y, por consiguiente, del volumen de tratamiento de datos personales de individuos en la red.

II. Sobre la revisión de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[2] Aquellos que a priori no ofrecen un nivel de protección adecuado de acuerdo con lo establecido en la Directiva 95/46/CE.

A la vista de lo anterior, la situación actual plantea de manera inevitable la cuestión de si la legislación puede afrontar plenamente algunos de los nuevos retos y modelos de negocio emergentes; especialmente la legislación tradicional, que tiene un ámbito geográfico de aplicación limitado y unas fronteras físicas que con Internet son inexistentes.

Hemos de tener en cuenta que, como pone de manifiesto el Profesor Lucrecio Rebollo Delgado, estamos en un periodo de evolución y perfeccionamiento constante de los derechos, como consecuencia directa del grado de democratización conseguido, y como resultado de ello, de la evolución tecnológica. Pero ocurre que son dos mundos contrapuestos. La tecnología es dinámica, siempre abre múltiples posibilidades y se expande tanto en el espacio como en el tiempo. El derecho por el contrario pretende lo estable, tiene fuertes limitaciones espaciales y temporales y muestra cierta pereza para la mutabilidad o la adecuación a las nuevas circunstancias. Pero inexorablemente se necesitan, su acoplamiento es imprescindible para la correcta ordenación social. Pero se constata que el derecho siempre va a remolque del desarrollo tecnológico, lo cual es lógico, porque atiende a solventar un problema, una necesidad social, que hasta que no se constata su existencia, no aparece la necesidad de su delimitación jurídica. De ello hemos de extraer otro presupuesto previo, y que se concreta en la imposibilidad o ineficaz que el ordenamiento jurídico prevea o limite la infinidad de posibilidades que ofrece la tecnología[3]

Por tanto, en principio parece que la respuesta a la cuestión de si la actual normativa regula con eficacia la garantía de los derechos fundamentales de las personas en los nuevos modelos de negocio en Internet, es negativa. Los modelos comerciales en Internet no encajan fácilmente con lo establecido en la Directiva 95/46/CE sobre protección de datos personales. La explotación de los datos efectuada a través de determinados servicios de las redes sociales, la indexación de información por los buscadores, la publicidad comportamental o el cloud computing requieren de cierta

[3] *Vid.* en sentido amplio, Rebollo Delgado Lucrecio, "El derecho a la propia imagen y la imagen como dato" en *Revista Española de Protección de Datos* nº 5, Julio-Diciembre 2008, pp 155-182 (Thomson-Civitas),

flexibilidad en la aplicación de las Directivas europeas y normas internas de los estados miembros frente al aparente "todo vale" de los EEUU u otros terceros países. Esta "flexibilidad" actualmente, y ante las escasas alternativas legales, en realidad consiste en dejar de lado el cumplimiento de las normas europeas para todo aquel que utiliza o contrata alguno de estos servicios a empresas ubicadas fuera del Espacio Económico Europeo.

En este sentido, es interesante destacar que ya en el año 2003 la sentencia del Tribunal de Justicia de la Unión Europea resolvió una cuestión planteada por el Göta hovrätt (Suecia), destinada a obtener, en el proceso penal seguido ante dicho órgano jurisdiccional contra Bodil Lindqvist, una decisión prejudicial sobre la interpretación de la Directiva 95/46/CE en relación con el alcance de algunos conceptos tal como el ámbito de aplicación de la Directiva, la publicación de datos personales en Internet, el lugar de la publicación de los datos, el concepto de transferencia de datos personales a países terceros y la libertad de expresión.

Según el citado Tribunal, si bien es cierto, que la conducta que consiste en hacer referencia en una página web a diversas personas por su nombre o por otros medios, constituye un tratamiento automatizado de datos personales en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE, no lo es menos que, no cabe presumir que el legislador comunitario tuviera la intención, en su momento, de incluir en el concepto de «transferencia a un país tercero de datos» la difusión de datos en una página web.

En esta línea el Tribunal de Justicia sostiene que, si de acuerdo con el artículo 25[4] de la Directiva 95/46/CE cada vez que se publican datos personales en una página web, se interpreta en el sentido de que existe una «transferencia a un país tercero de datos» dicha publicación de datos será forzosamente una transferencia a todos los países terceros en los que existen los medios técnicos necesarios para acceder a Internet. El régimen especial que prevé el capítulo IV de la citada Directiva se convertiría entonces necesariamente, por lo que se refiere a las operaciones en Internet, en un régimen de aplicación general. En efecto, en cuanto la Comisión detectara, con arreglo al artículo 25, apartado 4, de la Directiva 95/46, que un solo país tercero no garantiza un nivel de protección adecuado, los Estados miembros estarían obligados a impedir cualquier difusión de los datos personales en Internet.

Por ello y en este contexto, el Tribunal llega a la conclusión de que el artículo 25 de la Directiva 95/46 debe interpretarse en el sentido de que la publicación de datos en Internet no constituye, por sí misma, una «transferencia a un país tercero de datos» y

---

[4] Artículo 25. Principios. 1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.
2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.
3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.
4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.
5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.
6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.
Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

por tanto, no es necesario averiguar si alguna persona de un país tercero ha tenido acceso a la página web de que se trata o si el servidor del proveedor se encuentra físicamente en un país tercero.

A la vista está por tanto que, esta sentencia ya puso de relieve en el año 2003 la ineficacia de la aplicación de la Directiva 95/46/CE para proteger la privacidad y los derechos fundamentales de los ciudadanos europeos cuando el tratamiento de sus datos personales se lleva a cabo en Internet, desde una página o sitio alojado por un proveedor de servicios ubicado en la UE, de modo que dichos datos resultan accesibles a cualquier persona que se conecte a Internet, incluidas aquéllas que se encuentren en uno de los llamados terceros países.

Pese a ello y por contradictorio que pueda parecer, la Comisión Europea en su «Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)[5]» de 15 de mayo de 2003 –mismo año en que el Tribunal de Justicia de la Unión Europea resolvió el caso Lindqvist- consideró que no era necesaria la modificación de la Directiva en este momento. Dicha decisión además estuvo respaldada por la consulta realizada a la mayoría de los Estados miembros así como autoridades nacionales de control en materia de protección de datos.

Años más tarde, la misma posición es mantenida por la Comisión en su Comunicación al Parlamento Europeo y al Consejo, de 7 de marzo de 2007, «Seguimiento del Programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos»[6] donde se señala expresamente que, pese a que la Directiva se aplica en todos los Estados miembros, *se observa una creciente preocupación social en relación con el abuso y la mala utilización de datos personales en los sistemas de información en línea.*

---

[5] Fuente: Primer informe de la Comisión sobre la aplicación de la Directiva sobre protección de datos (95/46 CE) de 15 de mayo de 2003. Documento COM (2003) 265 final - no publicado en el Diario Oficial.

[6] Fuente: Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos. Documento COM (2007) 87 final no publicado en el Diario Oficial.

La Comisión consideró también en el citado informe que la Directiva *da forma al derecho fundamental a la protección de los datos personales; el respeto de sus normas garantiza la confianza de los individuos en la manera en que se utiliza su información, condición fundamental para el desarrollo de la economía que utiliza los medios electrónicos; establece una referencia para las iniciativas en una serie de áreas políticas; es tecnológicamente neutra y sigue proporcionando respuestas sólidas y apropiadas a estos asuntos*[7].

En base a lo anterior, la Comisión decidió que no era necesario presentar ninguna propuesta legislativa para modificar la Directiva.

Por fin, el 4 de noviembre de 2009, la Comisión Europea presentó su estrategia para el refuerzo de las normas de protección de datos en la UE, en todos los ámbitos de actuación política, incluido el del orden público, a la vez que se proponía como objetivo reducir la burocracia para las empresas y garantizar la libre circulación de datos en la UE.

La revisión del actual marco jurídico de protección de datos por parte de la Comisión, iniciada en el 2009 fue seguida de una consulta pública desarrollada hasta finales de ese mismo año y de otras más específicas a partes interesadas. La intención es modernizar las normas de protección de datos de la UE y se centra entre otros en los siguientes objetivos:

- Reforzar los derechos de las personas de modo que la recogida y uso de los datos personales se limite al mínimo necesario y se facilite una información clara sobre el tratamiento, así como la instrumentación adecuada del consentimiento cuando éste sea necesario, facilitando el ejercicio del "derecho al olvido".

---

[7] Fuente: Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos. Documento COM (2007) 87 final no publicado en el Diario Oficial.

- Potenciar la dimensión del mercado único mediante la reducción de los trámites burocráticos para las empresas y la garantía de la igualdad de condiciones en los distintos Estados Miembros, así como el establecimiento de pautas claras en materia de determinación de la jurisdicción competente.

- Garantizar niveles elevados de protección para los datos enviados fuera de la UE mediante la mejora y simplificación de los procedimientos de transferencia internacional de datos.

- Una aplicación más eficaz de las normas, reforzando y armonizando aún más el papel y los poderes de las autoridades de protección de datos, así como su cooperación y coordinación.

En la actualidad este proceso no ha terminado por lo que el nuevo marco legal europeo en materia de protección de datos personales no será aprobado a lo largo del año 2011.

III. La opinión del Grupo de Trabajo del artículo 29 y la Agencia Española de Protección de Datos.

El denominado Grupo de Trabajo del artículo 29[8] (órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad) no cuestiona los beneficios -tanto económicos como de servicio- que los nuevos modelos aportan, pero considera que muchas de las prácticas que éstos conllevan no debe realizarse a expensas de los derechos a la intimidad y a la protección de datos de las personas. Así, mantiene que el marco normativo de protección de datos de la UE, debe respetarse.

[8] Este Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad, compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión.

Por lo general este Grupo, analiza y aclara las obligaciones establecidas por el marco jurídico aplicable de la EU pero no prescribe el modo como deban cumplirse tales obligaciones desde el punto de vista técnico. En vez de ello, en diversas materias, el Grupo anima a la industria (y a otros agentes) a entablar el diálogo con vistas a promover medios técnicos o de otra índole para cumplir y armonizar el marco jurídico aplicable.

Entre los cometidos del programa de trabajo 2010-2011 del Grupo 29 se encuentra el análisis de cómo hacer frente a desafíos de los nuevos desarrollos tecnológicos, fundamentalmente cuestiones relacionadas con la globalización y a cambios institucionales resultantes del Tratado de Lisboa.

Otro de los objetivos del Grupo de Trabajo es aclarar y fortalecer el papel de todos los agentes en el ámbito de la protección de datos: las personas afectadas, los responsables del tratamiento de datos y las autoridades encargadas de la protección de datos. Se propone asimismo garantizar que el principio de «privacy by design» (consideración del derecho a la intimidad en la concepción de sistemas de tratamiento de datos) se integre en todas las áreas, lo que podría dar lugar a la implicación de nuevos agentes[9].

No obstante, en la actualidad y hasta que sea revisada la normativa vigente, Europa debe solucionar los conflictos jurídicos derivados de los nuevos modelos de negocio con la aplicación de las Directivas vigentes antes referidas. La cuestión que se plantea es cómo congenian estas últimas con el mercado global.

Por otro lado, nuestra autoridad de control, la Agencia Española de Protección de Datos (en adelante, AEPD), ha manifestado -en respuesta a la invitación de la Comisión sobre "un enfoque global de la protección de datos personales en el ámbito de la Unión Europea", que aunque el movimiento internacional de datos constituye uno de

[9] Fuente: Documento del Grupo del Artículo 29 00265/10/ES WP 170 "Programa de trabajo 2010 – 2011 Adoptado el 15 de febrero de 2010".

los mayores riesgos que el tratamiento de datos personales puede generar en la protección de la privacidad de las personas, sin embargo, resulta impensable el desarrollo y mantenimiento de un sistema como el actual, caracterizado por un importante componente de globalización.

En este sentido -según la AEPD- los avances tecnológicos como la "informática en la nube" o cloud computing, precisan de un instrumento análogo a las denominadas "Normas Empresariales Vinculantes", las cuales han supuesto en nuestro derecho interno -según el citado organismo- un elemento de flexibilización en lo que a la autorización de transferencias internacionales de datos en el seno de multinacionales se refiere. Para ello la Agencia aboga por la creación de un instrumento que tome como referencia los principios establecidos en la Decisión de la Comisión 2010/87/UE.

Además la AEPD, se posiciona por la inclusión en el futuro marco legislativo del denominado *"principio de rendición de cuentas"*, o *"accountability"*, de forma que el control previo de la adecuación podría recaer en el propio exportador de datos, reservándose el trámite burocrático de la autorización previa para aquellos supuestos en los que el riesgo para los interesados fuese especialmente elevado (movimientos internacionales de datos considerados especiales, por poner un ejemplo). De este modo, quien pretenda realizar la transferencia debería cerciorarse de que la misma se realiza con pleno respeto a las exigencias contenidas en la normativa europea, debiendo rendir cuentas frente a la autoridad de supervisión y frente a los propios interesados de que ha recabado todas las garantías necesarias para que la transferencia cumpla con el marco jurídico vigente y no perjudique los derechos e intereses de los interesados.

IV. Situación actual del cloud computing en el marco de las normas europeas.

Vamos a analizar la situación actual del "cloud computing" en el marco de las normas europeas y en particular en el marco de nuestro derecho interno teniendo en cuenta la caracterización de este negocio como un modelo basado en la continua

subcontratación de servicios y descentralización geográfica y transfronteriza de bases de datos que pueden almacenar información sobre individuos o personas físicas.

Partiremos no obstante del hecho, hasta ahora ya puesto de manifiesto, de que la normativa europea debe ser adaptada a las innovaciones surgidas en el sector de las comunicaciones electrónicas y nuevas tecnologías[10].

Por otro lado, tal y como señala el "Dictamen 8/2010 sobre el Derecho aplicable emitido por el Grupo 29 el 16 de diciembre de 2010", definir el régimen jurídico aplicable al tratamiento de datos personales de conformidad con la Directiva 95/46/CE constituye una cuestión clave por diversas razones. Entre ellas, porque determinar el marco jurídico de la UE respecto del tratamiento de datos personales sirve para aclarar también cuál es el marco jurídico internacional y los límites de ambos. Una percepción clara del Derecho aplicable contribuye –según dispone el Dictamen- a garantizar, no solo la seguridad jurídica a los responsables del tratamiento, sino también a las personas y otras partes interesadas.

Sin entrar en el debate de la determinación del derecho aplicable, vamos directamente a abordar el requisito regulatorio fundamental que ha establecido la UE respecto de la situación de hecho creada por el cloud computing.

Como es bien sabido, el cloud computing constituye un negocio donde el cliente -responsable de los tratamientos y ficheros que contienen datos personales- contrata la prestación de servicios que implican un acceso a los datos personales a un tercero, quien a su vez inicia una subcontratación "en cadena" con otros terceros. En definitiva se lleva a cabo la sucesiva realización de tratamientos por encargo pudiendo ocurrir que alguno o todos los proveedores que prestan el servicio estén ubicados fuera del territorio de la UE o dicho de otra manera, en uno de los llamados terceros países.

---

[10] Aunque esto será un hecho a corto o medio plazo, cierto es que en un sector como el tecnológico la rápida evolución de la industria siempre dejará de manifiesto un cierto desfase con la aplicación de las normas legales, cuyos procesos de elaboración y aprobación son lentos y muy burocráticos y su finalidad la regulación de situaciones generales y no casuísticas concretas.

Para que la sucesiva contratación de servicios sea legítima y acorde al ordenamiento jurídico europeo, el cliente o responsable del fichero y tratamientos afectados queda obligado a suscribir un contrato donde se disponga expresamente que dicho prestador de los servicios (al que se denomina encargado del tratamiento) solo actúa siguiendo las instrucciones del responsable del fichero o tratamiento que es objeto del servicio.

Cuando el prestador de servicios además se encuentra en un tercer país, como requisito adicional a la suscripción del contrato será preciso obtener la autorización de la autoridad de control correspondiente, en España, la AEPD.

A través del contrato de acceso a datos –acompañado cuando corresponda de las autorizaciones de las autoridades de control de cada Estado miembro- el responsable del fichero establecido en un país miembro de la UE traslada sucesivamente a los distintos prestadores de servicio que intervienen en el cloud computing, las condiciones y garantías que deben adoptar para garantizar el nivel de protección adecuado de acuerdo con la Directiva 95/46/CE. Se deja a las partes únicamente plena libertad, para decidir sobre las cuestiones relacionadas con sus negocios y siempre que dichas cuestiones no contradigan las cláusulas contractuales que regulen condiciones y garantías en materia de protección de datos personales de acuerdo con la citada Directiva.

Ligado a lo anterior, se encuentra la obligación del prestador de los servicios de ofrecer garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas respecto de los datos personales objeto del servicio. Así, cualquier prestador de servicios de cloud computing -sea cual sea el lugar que ocupe en las sucesivas subcontrataciones- deberá aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados y contra cualquier otro tratamiento ilícito de datos personales.

De acuerdo con la Directiva 95/46/CE, dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse. Pero una cuestión importante en esta materia es que la Directiva no concreta cuáles son estas medidas de seguridad que, en todo caso, deberán ser pactadas entre las partes.

En cuanto a la forma del llamado contrato de acceso a datos, habrá que atender fundamentalmente a lo establecido en la "Decisión de la Comisión de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo" cuando la entidad responsable del tratamiento (exportador de los datos) contrata a un prestador de servicios ubicado en un tercer país quien a su vez procede a la subcontratación de otro prestador de servicios también ubicado en un tercer país. Es decir, el supuesto de hecho de aplicación de la Decisión de 5 de febrero supone 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.

En base a lo anterior, dicha Decisión no se aplica a la situación en la que la entidad responsable del tratamiento contrata con un encargado del tratamiento establecido en la UE quien a su vez subcontrata sus operaciones de tratamiento a un tercer encargado del tratamiento (también llamado en el argot jurídico "subencargado" por tratarse de la segunda subcontratación y/o subsiguientes) establecido en un tercer país. En tales situaciones, según la normativa europea, los Estados miembros son libres de imponer -a través de sus legislaciones internas- al responsable del fichero, el uso de las cláusulas contractuales tipo establecidas en la Decisión para llevar a cabo la contratación del segundo encargado del tratamiento (o subencargado) establecido en el tercer país. En pura lógica y siendo críticos, no parece que ello tenga sentido puesto que se deja a la discrecionalidad de los órganos de control europeos la forma de garantizar los derechos de las personas pudiendo unos países establecer discriminatoriamente para las empresas, unos requisitos más flexibles que en otros países de la UE.

De hecho, en España como exigencia adicional la AEPD exige que el responsable del fichero sea siempre parte contractual firmante del contrato con cualquier subencargado del tratamiento ubicado en el tercer país, lo cual no es viable en la mayoría de las situaciones que se dan en la práctica.

Si a grandes rasgos estas son las previsiones legales que exige la normativa de la UE cabe preguntarse dónde está el problema de los servicios del cloud computing en materia de protección de datos en un marco "aparentemente" tan claro.

Bien, podríamos decir que el problema no es que el marco legal no sea claro, sino que es complicado en su cumplimiento o ejecución. Dicho de otro modo, son las consecuencias legales del modelo de negocio lo que dificulta en Europa su expansión. Veamos a continuación la causa.

Situándonos en el marco de la Decisión de la Comisión de 5 de febrero de 2010, como obligaciones del cliente responsable de los ficheros y exportador de datos, entre otras, resultan las siguientes:

- Garantizar que el tratamiento de los datos personales, incluida la propia transferencia, ha sido efectuado y seguirá efectuándose de conformidad con las normas pertinentes de la legislación de protección de datos aplicable (y, si procede, se ha obtenido la autorización del órgano de control del Estado miembro de establecimiento del exportador de datos para llevar a cabo la transferencia);

- Proporcionar al prestador del servicio (importador de datos) tanto al inicio como durante la prestación de los servicios de tratamiento de los datos personales, instrucciones para que el tratamiento de los datos personales transferidos se lleve a cabo exclusivamente en nombre del exportador de datos y de conformidad con la legislación de protección de datos aplicable.

- Exigir al importador de datos garantías suficientes en lo que respecta a las medidas de seguridad técnicas y organizativas especificadas a través de un anexo al contrato;

- Verificar que, de conformidad con la legislación de protección de datos aplicable, dichas medidas resultan apropiadas para proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizados, especialmente cuando el tratamiento suponga la transmisión de los datos por redes, o contra cualquier otra forma ilícita de tratamiento y que dichas medidas garantizan un nivel de seguridad apropiado a los riegos que entraña el tratamiento y la naturaleza de los datos que han de protegerse, habida cuenta del estado de la técnica y del coste de su aplicación;

- Asegurar que dichas medidas se lleven a la práctica;

- Si la transferencia incluye categorías especiales de datos, se debe informar a los interesados, antes de que se efectúe la transferencia, o en cuanto sea posible, de que sus datos podrían ser transferidos a un tercer país que no proporciona la protección adecuada en el sentido de la Directiva 95/46/CE;

- Poner a disposición de los interesados, previa petición de estos, una copia de las cláusulas y una descripción sumaria de las medidas de seguridad, así como una copia de cualquier contrato para los servicios prestados por cualquier encargado del tratamiento sea cual sea el puesto que ocupe en la cadena de subcontrataciones (lo cual por tanto incluye a todos los subencargados del tratamiento contratados por el primer encargado del tratamiento y principal) con excepción de las cláusulas que contengan información comercial que podrán ser eliminadas.

- Garantizar que, en caso de existir más de un encargado del tratamiento, todos los subsiguientes al primero (es decir todos los subencargados del

tratamiento) ejecutarán cualquier actividad de tratamiento de datos al menos el mismo nivel de protección de los datos personales y los derechos de los interesados que el importador de datos o responsable del fichero;

Como obligaciones del prestador del servicio o importador de datos, entre otras, resultan las siguientes:

- Tratar los datos personales transferidos solo en nombre del exportador de datos, de conformidad con sus instrucciones y las cláusulas. En caso de que no pueda cumplir estos requisitos por la razón que fuere, deberá informar de ello sin demora al exportador de datos, en cuyo caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato;

- Garantizar la inexistencia de motivos para creer que la legislación que le es de aplicación le impida cumplir las instrucciones del exportador de datos y sus obligaciones a tenor del contrato y que, en caso de modificación de la legislación que pueda tener un impotente efecto negativo sobre las garantías y obligaciones estipuladas, notificará al exportador de datos dicho cambio en cuanto tenga conocimiento de él, en cuyo caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato;

- Garantizar que ha puesto en práctica las medidas de seguridad técnicas y organizativas acordadas con el exportador responsable del tratamiento;

- Tratar adecuadamente en los períodos de tiempo prescritos todas las consultas del exportador de datos relacionadas con el tratamiento que se esté realizando de los datos personales sujetos a transferencia y atender a la opinión de la autoridad de control en lo que respecta al tratamiento de los datos transferidos;

- Ofrecer a petición del exportador de datos sus instalaciones de tratamiento de datos para que se lleve a cabo la auditoría de las actividades de

tratamiento cubiertas por las cláusulas. Esta será realizada por el exportador de datos o por un organismo de inspección, compuesto por miembros independientes con las cualificaciones profesionales necesarias y sujetos a la confidencialidad, seleccionado por el exportador de datos y, cuando corresponda, de conformidad con la autoridad de control;

- Poner a disposición de los interesados, previa petición de estos, una copia de las cláusulas, o de cualquier contrato existente para el subtratamiento de los datos, a menos que las cláusulas o el contrato contengan información comercial, en cuyo caso podrá eliminar dicha información comercial, así como proporcionar igualmente una descripción sumaria de las medidas de seguridad, en aquellos casos en que el interesado no pueda obtenerlas directamente del exportador de datos;

- Garantizar que, en caso de subtratamiento de los datos, habrá informado previamente al exportador de datos y obtenido previamente su consentimiento por escrito;

- Enviar sin demora al exportador de datos una copia de cualquier acuerdo con el subencargado del tratamiento que concluya.

En cuanto al régimen de responsabilidad previsto en la Decisión de 5 de febrero de 2010 resulta destacable la obligación para las partes -cliente y prestador del servicio de cloud computing- de acordar que los interesados que hayan sufrido daños como resultado del incumplimiento de las obligaciones mencionadas en el contrato por cualquier subencargado del tratamiento tendrán derecho a percibir una indemnización del exportador de datos para el daño sufrido.

En el caso en que el interesado no pueda interponer contra el exportador de datos la demanda de indemnización por incumplimiento por parte del importador de datos o su subencargado de sus obligaciones -por haber desaparecido *de facto*, cesado de existir jurídicamente o ser insolvente- el importador de datos debe aceptar contractualmente

que el interesado pueda demandarle a él en el lugar del exportador de datos, a menos que cualquier entidad sucesora haya asumido la totalidad de las obligaciones jurídicas del exportador de datos en virtud de contrato o por ministerio de la ley, en cuyo caso los interesados podrán exigir sus derechos a dicha entidad.

Además la Decisión no permite al importador de datos basarse en un incumplimiento de un subencargado del tratamiento de sus obligaciones para eludir sus propias responsabilidades.

En definitiva como puede comprobarse, obtener la firma de un contrato según el modelo de la Decisión de 5 de febrero de 2010 no se presenta como una cuestión sencilla si además tenemos en cuenta que normalmente las empresas de la industria prestadoras de servicios de cloud computing suelen adelantar sus condiciones contractuales mediante cláusulas de adhesión innegociables y en la mayoría de los casos con exoneraciones y limitaciones de responsabilidad completamente abusivas y alejadas de cualquier garantía de los derechos de los interesados.

Es una obviedad que el hecho mismo de que exista una cadena de subcontrataciones transfronteriza aumenta la problemática relativa a la pérdida del control sobre los distintos subcontratistas, su identificación, lugar de residencia y por tanto aumenta la posibilidad de que el contrato no llegue a firmarse en ningún caso.

Lo anterior no deja de ser una causa que también trae como consecuencia la pérdida de control por el responsable del tratamiento sobre la implantación de medidas de seguridad técnicas y organizativas (o de cualquier naturaleza) que el encargado del tratamiento debe realizar con el fin de proteger los datos personales. Este control se pierde incluso en los primeros eslabones de la cadena de subcontratistas si no se sigue un estricto protocolo.

V. Situación actual del cloud computing en el marco de nuestro derecho interno.

Centrando nuestra atención en el marco legal interno en España podemos comprobar que la situación es ciertamente algo más compleja que en algunos otros países de la UE por dos motivos: la elevada cuantía de las sanciones económicas que impone la legislación española por la infracción de la normativa interna; y los excesivos formalismos y rigideces jurídicas que se derivan del título VIII "de las medidas de seguridad en el tratamiento de datos de carácter personal" del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Así, de acuerdo con la Ley Orgánica 15/1999 de protección de datos de carácter personal vigente en España, se califica como leve la infracción consistente en llevar a cabo la transmisión de los datos a un encargado del tratamiento sin dar cumplimiento a los deberes formales consistentes en la firma de un contrato de acceso a datos. Asimismo, se califica como muy grave la infracción consistente en llevar a cabo la transferencia internacional de datos de carácter personal con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la AEPD salvo en los supuestos en los que conforme a esta Ley y sus disposiciones de desarrollo dicha autorización no resulta necesaria. En el primer caso la infracción está sancionada con multa de 900 a 40.000 euros. En el segundo, la infracción está sancionada con multa de 300.001 a 600.000 euros.

Si además nos encontramos en el sector de la Administración Pública y prestación de servicios públicos (actualmente inmerso en grandes cambios tecnológicos ante la implantación de la denominada "Administración Electrónica"), la situación se agrava en lo que a la rigidez y complejidad de los procedimientos de contratación de contratación se refiere.

La necesaria adhesión a los pliegos administrativos de contratación pública, que a todos los efectos conforman el contrato administrativo con el ente público, y la imposibilidad de negociación de las condiciones de ejecución impiden seguramente a todas luces el cumplimiento de los requisitos anteriormente contemplados por el

adjudicatario en la futura prestación de servicios de cloud computing y la adecuación de los mismos a la Decisión de 5 de febrero de 2010, dejando por tanto más vulnerables los derechos de los ciudadanos cuyos datos son objeto de tratamiento y expuestas a las empresas privadas que contraten con la Administración a severas multas económicas.

Esta situación es aún más grave cuando la prestadora de los servicios de cloud computing es una administración respecto de otras terceras, por ejemplo el caso de una diputación que proporciona servicios a los ayuntamientos, para lo cual a su vez la diputación prestadora de servicios seguramente subcontrará los servicios de cloud computing a otras terceras entidades privadas iniciándose así la cadena de subcontrataciones sin garantías ni control.

Ahora la pregunta que cabe hacer es, ¿debe la UE adaptarse a los imperativos del desarrollo de Internet y los negocios en línea o debe ser Internet, las tecnologías y los negocios en línea quienes se adapten a las normas europeas para garantizar su cumplimiento?.

VI. Conclusiones e impactos.

Las tecnologías y los negocios emergentes como el cloud computing son una realidad imparable. En este negocio -como en otros muchos- no se ha conseguido alcanzar la plena aplicabilidad de la Directiva 95/46/CE, y manifestar lo contrario sería una falacia.

Asimismo, se hace preciso el juicio de valor sobre, si como parece, la Directiva 95/46/CE constituye un marco jurídico general que cumple con sus objetivos originales y además es una garantía suficiente para el funcionamiento del mercado interior asegurando al mismo tiempo un alto nivel de protección o por el contrario, se ha convertido en un obstáculo para las relaciones comerciales entre UE y los llamados terceros países.

Aparentemente la respuesta es que la Directiva 95/46/CE se ha convertido en una traba para las relaciones entre Europa y los llamados terceros países por lo cual, la Comisión Europea ya ha iniciado los pasos necesarios para aproximar la regulación legal a la realidad social y tecnológica en una difícil misión que, ciertamente, no tiene visos de prosperar satisfactoriamente para todas las partes interesadas.

Por el momento y hasta que la Comisión Europea lleve a cabo los cambios oportunos -sea cual sea la dirección de los mismos- la situación en la que nos encontramos en nuestro derecho interno es jurídicamente insegura y empresarialmente arriesgada.

- Desde el punto de vista de la seguridad jurídica, la falta de regulación por las normas europeas de todos los supuestos de hecho que pueden darse en el marco de las transferencias internacionales de datos, ha provocado que cada país establezca sus propios protocolos y procedimientos. Particularmente en España, donde la situación es la misma, únicamente fue abordado un intento de armonización a través de la "Instrucción 1/2000 de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos" que resultó declarada nula en buena parte por la sentencia de la Audiencia Nacional de 15 de Marzo de 2002 *al pretender extender su aplicación a las transferencias internacionales de datos comprendidas en los supuestos de excepción contemplados en la Ley Orgánica 15/1999 de protección de datos de carácter personal*. Desde entonces, y al margen del reglamento de desarrollo de la Ley Orgánica de protección de datos de carácter persona, la AEPD solo ha abordado iniciativas para estudio de la situación pero no ha informado ni emitido dictámenes, instrucciones ni recomendaciones suficientemente estables y justificadas.

- Desde el punto de vista del riesgo empresarial y partiendo de la situación de inseguridad jurídica ya mencionada, las empresas y

> administraciones públicas españolas no pueden abandonar el barco del "progreso tecnológico" y por tanto se arriesgan a contratar servicios de cloud computing sin los debidos protocolos y garantías legales. En muchos casos la contratación se lleva a cabo vía servicios web y las empresas solicitantes de servicios únicamente se adhieren a las condiciones generales de servicio ofrecidas por el proveedor sin posibilidad de negociación ni inclusión de las garantías exigidas por nuestra normativa; pero aún cuando la contratación no sea vía web sino negociada, existe una manifiesta incapacidad para firmar los contratos de acceso a datos que propone tanto nuestro derecho interno como la UE porque los proveedores ubicados en terceros países no están dispuestos a aceptar las cláusulas de responsabilidad que estos conllevan ni el cumplimiento de la rígida normativa europea. Con ello las empresas españolas cuando contratan estos servicios, en muchas ocasiones prescinden en primer lugar, de la autorización que deben solicitar a la AEPD asumiendo una infracción administrativa sancionable con multa de 300.001 a 600.000 euros y en segundo lugar, de la firma del contrato de acceso a datos sancionable con multa entre 600 y 40.000 euros. En todo caso, un riesgo que a muchas empresas españolas podría llevar al cierre.

A mayor abundamiento, no es una cuestión baladí preguntarse qué ocurriría si un ciudadano español solicitase información a una empresa o administración pública que hubiera contratado "servicios en la nube" sobre sus datos personales, los contratistas y subcontratistas que tienen acceso a los mismos, el contenido no comercial de los contratos de servicio firmados en su caso y la memoria de las medidas de seguridad que cada uno de estos agentes debe garantizar. De acuerdo con la normativa vigente este ciudadano estaría en su derecho de obtener copia de toda esta información en los casos en que fuera de aplicación la Decisión de 5 de febrero de 2010 y de no recibirla, se encontraría en su derecho de denunciar ante la AEPD que su derecho no ha sido debidamente atendido, quedando dicho organismo obligado a resolver.

Y frente a ello la industria de los terceros países no parece sensibilizada con el problema que sufre Europa, seguramente porque el problema *"aún no es suyo"*. En definitiva, si pese a no aceptar el cumplimiento de la normativa de la UE, desde Europa se siguen contratando sus servicios, efectivamente parece que la industria de los terceros países no tiene ningún problema.

Quizás la solución pasa porque la industria europea se proponga la creación de grandes plataformas para la prestación de servicios de cloud computing, adecuadas y garantistas de los derechos establecidos en las distintas directivas y decisiones aplicables. Aunque por el momento, la rigidez normativa sitúa a Europa y a su industria en una posición de clara desventaja competitiva frente al desarrollo de modelos de negocio por la industria de los terceros países.

La cuestión es, si rebajando las exigencias legales establecidas por la Directiva 95/46/CE y las decisiones que regulan las transferencias internacionales de datos a terceros países, sería posible mantener los requisitos de seguridad en las prestaciones y las garantías que protegen los derechos de las personas. A priori parece que la seguridad tecnológica está garantizada, no es por tanto un problema de seguridad técnica lo que dificulta las relaciones entre los diversos actores que operan en las relaciones de cloud computing, sino un problema de seguridad legal.

Quizás la pregunta final es hacia dónde debería caminar Europa.

VII.-Bibliografía y documentación consultada.

Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 7 de marzo de 2007, «Seguimiento del Programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos» COM (2007) 87 final - no publicado en el Diario Oficial.

Documento del Grupo del Artículo 29 sobre protección de datos 00265/10/ES - WP 170 "Programa de trabajo 2010 – 2011" adoptado el 15 de febrero de 2010.

Informe de la Comisión, de 15 de mayo de 2003, «Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE)» COM (2003) 265 final - no publicado en el Diario Oficial.

REBOLLO DELGADO LUCRECIO, (2008), "El derecho a la propia imagen y la imagen como dato" *en Revista Española de Protección de Datos* nº 5, Julio-Diciembre 2008, pp 155-182 (Thomson-Civitas).

ANA MARÍA MARZO PORTERA. Licenciada en Derecho especialidad empresa por la Universidad de Valencia. Colegiada en el Ilustre Colegio de Abogados de Madrid.

En la actualidad es socio director del despacho de abogados EQUIPO MARZO especializado profesionalmente en el marco legal sobre protección de datos, comercio electrónico, administración electrónica, propiedad intelectual, contratación informática, seguridad de la información y publicidad online.

Autora del manual *Guía Práctica para la Protección de Datos de Carácter Personal,* Ediciones Experiencia, 2009.

Coautora de los siguientes manuales: *Normativas de obligado cumplimiento para la empresa sobre protección de datos,* Diario Expansión y Grupo Wolters Kluwer, 2009; *La auditoría de seguridad en la protección de datos de carácter personal,* Ediciones Experiencia, 2009; *Vigilancia y control de las comunicaciones electrónicas*

en el lugar de trabajo, Ediciones Experiencia, 2009; *Todo sobre el nuevo reglamento de la protección de datos,* SODENA (Sociedad de desarrollo de Navarra), 2008; *Guía Práctica sobre protección de datos de carácter personal para Abogados,* Grupo Difusión, 2008; E*studio práctico sobre la protección de datos de carácter personal,* Editorial: Lex Nova 2007; *La contratación por vía electrónica,* ANETCOM, 2006; *La Auditoría de seguridad en la protección de datos de carácter personal*, Ediciones Experiencia, 2004; *Los contratos informáticos y electrónicos. Guía práctica y formularios.* Ediciones Experiencia, 2004, *La protección de datos en la gestión de empresas,* Aranzadi, S.A, 2004; *Internet, claves legales para la empresa* Civitas, 2002.

Ha participado como profesora en los siguientes cursos y Master: Master oficial sistemas y servicios en la sociedad de la información (2010-2009-2008 Universidad de Valencia); Taller práctico sobre redes sociales y protección de datos en el grado de derecho (2010, Universidad Europea de Madrid UEM); Master de Propiedad Industrial, Intelectual y Nuevas Tecnologías (2008-2007, Madrid, Fundación EOI Escuela de Negocios); *Curso practico sobre las implicaciones de la Ley de Protección de datos* (2005, Alicante, Escuela de Negocios de la Universidad de Alicante); *Master en Derecho de las Nuevas Tecnologías* (2004-2003-2002-2001, Madrid Escuela Internacional de Negocios Aliter); *Master Net-Economía y Dirección de Empresas* (2004-2003- 2002-2001 Madrid, Centro Villanueva adscrito a la Universidad Complutense de Madrid); *Curso de Especialista Derecho de las Tecnologías de la Información y de Comunicaciones* (2003-2002-2001, Valladolid en Foro Empresarial para el desarrollo Europeo); *Master de Gestión Portuaria Fundación IPEC y Autoridad Portuaria de Valencia* (2001); *Master de Legislación de Internet* (2000, Santiago de Compostela, Centro Europeo Atlántico); *III Curso especializado de derecho de las telecomunicaciones y tecnologías de la información* (Septiembre-Noviembre 2000, Recoletos conferencias y formación); *Master en Marketing y Comunicación Multimedia* (1999, Madrid, IEDE Institute for Executive Development); *Master en Informática y Derecho* (1998-1999 Madrid, Universidad Complutense de Madrid-Asociación Multisectorial de Empresas Españolas de Electrónica); *Monográfico Comercio Electrónico y Derecho de las Nuevas Tecnologías* (1999-1998, Madrid, Centro de

estudios financieros); *Curso de especialización "Derecho Informático"* (1996-1995-1994, Madrid, Universidad Carlos III).

Profesora del written Course *"Tratamiento de datos y normativa aplicada a la Videovigilancia: Aspectos jurídico prácticos de la videovigilancia",* curso práctico on line IIR España, 24 de Octubre de 2008.

Además, es autora de diferentes artículos, notas, y comentarios publicados en Revistas jurídicas, técnicas y de asociaciones y ponente habitual en numerosos foros profesionales organizados en España sobre protección de datos, propiedad intelectual, comercio electrónico y administración electrónica, entre otros.