IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

http://idp.uoc.edu

Monográfico «VI Congreso Internet, Derecho y Política. *Cloud Computing*: El Derecho y la Política suben a la Nube»

ARTÍCULO

¿Quién controla la nube?

Ronald Leenes

Fecha de presentación: julio de 2010
Fecha de aceptación: septiembre de 2010
Fecha de publicación: diciembre de 2010

Resumen
Este artículo trata sobre algunos de los temas de protección de datos que se cuestionan en computación en nube. Concretamente, aborda la cuestión de la responsabilidad en el tratamiento de datos personales en situaciones de computación en nube. Aborda esta cuestión desde la perspectiva de la Unión Europea. ¿Cómo deben evaluarse modelos de computación en nube diferentes por lo que respecta a la Directiva 95/46/CE? y ¿siguen siendo útiles los conceptos de responsable del tratamiento de datos, encargado del tratamiento de datos e interesado o titular de los datos tal como se definen en esta Directiva? La conclusión de este análisis es que las situaciones de computación en nube se tienen que evaluar de forma individual y que la protección que se ofrece a los titulares de los datos o interesados en la Directiva suele ser insatisfactoria.

Palabras clave
computación en nube, privacidad, protección de datos

Tema
Computación en nube

Who Controls the Cloud?

Abstract
This article addresses some of the data protection issues at stake in cloud computing: more specifically the question of responsibility regarding personal data processing in cloud computing scenarios from an EU perspective. How are the different schemes to be assessed in light of Directive EU/95/46? And are the notions of data controller, data processor, and data subject, as defined in this Directive, still useful? The conclusion of this analysis is that cloud computing scenarios have to be assessed on an individual basis and that the protection the Directive offers to data subjects is often unsatisfactory.

Keywords
cloud computing, privacy, data protection

Theme
Cloud computing

Introducción

Cada cierto tiempo, la industria de la informática se ve sacudida por un nuevo paradigma. En los años sesenta y setenta, se conectaban terminales simples a ordenadores centrales, en los años ochenta, el PC hizo que el trabajo pasara del ordenador central al ordenador personal. En los años noventa, fuimos testigos de la adopción de Internet a gran escala, que no solo permitió a la gente ir más allá de su PC y aventurarse en la *world wide web*, sino que también hizo posible la reconexión con los ordenadores centrales y la infraestructura informática de la empresa. A principios del nuevo milenio, la computación en red parecía que iba a ser el siguiente paso, pero hoy este concepto se ha visto eclipsado por la computación en nube. Para algunos, la computación en nube es revolucionaria: «Estamos entrando en un mundo nuevo. Un mundo de aplicaciones de próxima generación y plataformas de próxima generación»,[1] mientras que otros son mucho más cautos: «Las nubes son vapor de agua. [...] Esto no es más que un ordenador conectado a una red.»[2] El analista de empresas Gartner parece estar de acuerdo con esto último y afirmó que la computación en nube está en la cima de las «expectativas infladas», y de camino al «valle de la desilusión».[3]

Independientemente de si la computación en nube va cambiar o no radicalmente el panorama de la computación, esta ya es un hecho en la vida de muchos empresarios, empleados, clientes y ciudadanos. Los servicios y, de hecho, plataformas enteras de computación se transfieren a «la nube», lo que significa que la ubicación del almacenamiento de datos y el procesamiento de los datos se vuelven conceptos difíciles de definir. En lugar de tener los datos almacenados en bases de datos propias de la empresa o en el propio PC del usuario, los datos en entornos de computación en nube pueden estar en cualquier parte del mundo. Y peor aún, los datos pueden trasladarse en un instante de un país a otro por razones de eficiencia. En efecto, los datos están en la nube. Esto plantea numerosos problemas jurídicos en materia de protección de datos, confidencialidad, propiedad intelectual etc.[4] La computación en nube, por su naturaleza, también cuestiona los fundamentos de la normativa de protección de datos que se basa en la idea de que los datos personales son tratados por responsables del tratamiento de datos cuya ubicación se supone conocida (Leenes, 2008b, pág. 360). La Directiva 95/46/CE sobre protección de datos[5] (en adelante DPD) trató de establecer las normas para el procesamiento de datos personales con los (grandes) sistemas informáticos que residen en las empresas y los gobiernos. El modelo de la computación en nube podría no encajar con este modelo.

Este artículo trata sobre algunos de los temas de protección de datos que se cuestionan en computación en nube. Concretamente, se aborda la cuestión de la responsabilidad en el tratamiento de datos personales en situaciones de computación en nube. Trataré esta cuestión desde la perspectiva de la Unión Europea. ¿Cómo deben evaluarse modelos de computación en nube diferentes por lo que respecta a la Directiva 95/46/CE? y ¿siguen siendo útiles los conceptos de responsable del tratamiento de datos, encargado del tratamiento de datos e interesado o titular de los datos tal como se definen en esta Directiva?

La estructura de este artículo es la siguiente. En primer lugar, haré un breve resumen de los conceptos fundamentales en el ámbito de la computación en nube. A continuación, describiré brevemente la Directiva 95/46/CE, centrándome en los conceptos de datos de carácter personal, interesado, responsable del tratamiento de datos y encargado del tratamiento de datos. A continuación, evaluaré diferentes situaciones de computación en nube a la vista de estos conceptos. La conclusión de este análisis será que las situaciones de computación en nube se tie-

1. Marc Benioff de Salesforce. Ver: http://www.zdnet.com/blog/btl/salesforces-benioff-clouds-arent-in-a-box/39488
2. Larry Ellison, de Oracle, en la misma conferencia en la que Benioff ensalzó la computación en nube. Ver: http://venturebeat.com/2009/10/01/larry-ellisons-annual-cloud-computing-smackdown/ for his entire speech.
3. Ver: http://www.readwriteweb.com/archives/gartner_hype_cycle_2010_cloud_computing_at_the_pea.php
4. Para una descripción general de los problemas legales, véase por ejemplo Catteddu y Hogben, 2009 y Van Gyseghem y otros, 2010.
5. Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea, del 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, DO N.º L 281 del 23 de noviembre de 1995.

nen que evaluar de forma individual y que la protección que se ofrece a los interesados en la Directiva suele ser insatisfactoria. Por tanto, los usuarios de los servicios de computación en nube quizá quieran recurrir a contratos y acuerdos de nivel de servicio con el fin de mitigar algunos de los riesgos. Por último, se incluirán algunas conclusiones y recomendaciones.

Computación en nube

La computación en nube es un concepto difícil de precisar. Abarca una gran variedad de modelos de servicios y modelos de aplicación. No parece existir una definición establecida, aunque la definición del NIST parece que lleva camino de convertirse en la definición *de facto*: «La computación en nube es un modelo para permitir el acceso conveniente por red bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden proporcionarse y servirse rápidamente con un esfuerzo mínimo de gestión o interacción por parte del proveedor del servicio.» (Meil y Grance, 2009). Para nuestros propósitos, solo hay que destacar unos cuantos aspectos. Los más importantes son el hecho de que los recursos informáticos del proveedor se reúnen para servir a varios consumidores con un modelo multiarrendatario.

Los diferentes recursos físicos y virtuales se asignan y reasignan dinámicamente según la demanda de los consumidores. En general, el cliente no tiene ningún control o conocimiento sobre la ubicación exacta de los recursos asignados, pero puede llegar a especificar la ubicación a un nivel más alto de abstracción (por ejemplo, país, estado, o centro de datos) (Meil y Grance, 2009).

Los servicios de computación en nube incluyen recursos como el almacenamiento, procesamiento, memoria, ancho de banda de red y máquinas virtuales. En general, se distinguen tres tipos de servicios: software como servicio (SaaS) en nube, plataforma como servicio (PaaS) en nube e infraestructura como servicio (IaaS) en nube. En el caso del SaaS, el consumidor usa una aplicación que le proporciona el proveedor de la nube. Google Docs, Hotmail de Microsoft y Dropbox son ejemplos conocidos. En el caso de la PaaS, el proveedor de servicios en nube ofrece una plataforma para el desarrollo de aplicaciones o servicios en la que los clientes pueden crear su propia aplicación o servicio. Un ejemplo es Vtravelled, un servicio de viajes desarrollado por Virgin Atlantic que se ejecuta en la plataforma Amazon AWS.[6] Por último, la infraestructura como un servicio permite a los clientes ejecutar cualquier software, sistemas operativos y aplicaciones incluidos, en el equipo del proveedor de servicios. En cuanto a modelos de aplicación, se hace una distinción en infraestructuras operadas por una sola organización (nube privada), nube de infraestructuras compartidas por varias organizaciones y que apoya a una comunidad específica con intereses comunes (nube de la comunidad), las infraestructuras públicas y las nubes híbridas. Obviamente, los clientes tienen más control en las nubes privadas que en las nubes públicas, que por su naturaleza deben tener términos y condiciones generales.

Para este trabajo, voy a usar algunos ejemplos sencillos para ilustrar el análisis. Los casos difieren en si se trata de nubes públicas o privadas, en la ubicación de tratamiento y almacenamiento de datos y en la medida en la que el usuario final tiene control sobre el servicio ofrecido. Voy a limitar el análisis a los casos de SaaS, ya que ilustran bien las complejidades de la regulación por lo que respecta a los diferentes actores y ofertas de servicios. El primer ejemplo es el de Eleni Primero, estudiante de la Universidad de Tilburg, una institución que recientemente ha decidido usar el entorno Microsoft Live@Edu[7] para sus estudiantes. En este caso, los servidores alojados en la Unión Europea (en Amsterdam, con una copia de seguridad en Irlanda) prestan el servicio.[8] Este es un ejemplo de SaaS privada.

6. Véase http://www.vtravelled.com
7. Véase http://www.microsoft.com/liveatedu/free-email-accounts.aspx?locale=en-US&country=US
8. Este fue un factor importante para la Universidad de Tilburg para elegir a Microsoft en lugar de a su rival Google, que no podía garantizar la ubicación de los servidores. Véase, si se quiere información sobre problemas similares, las dudas de Yale para cambiar a Google mail, http://www.yaledailynews.com/news/university-news/2010/03/30/its-delays-switch-gmail-community-input/

El segundo caso es el del profesional que usa Google Docs y otras aplicaciones de Google para colaborar con sus socios en un proyecto europeo. Este es un ejemplo de SaaS pública. Google no puede especificar la ubicación de los servidores para este caso de uso particular.

El tercer caso es el de Tim Third, que tiene un perfil de Facebook que está alojado en una SaaS pública probablemente situada en los Estados Unidos.

En cada modelo de computación en nube podemos distinguir diferentes entidades:

- El proveedor de servicios de computación en nube (CCS), es decir, la persona física o jurídica que presta el servicio (SaaS, IaaS o PaaS) en un sistema de computación en nube.
- El abonado o cliente, es decir, la persona física o jurídica que suscribe un contrato con el proveedor de servicios de computación en nube. El abonado puede ser una persona, como Tim, o una organización, como la Universidad de Tilburg.
- El usuario (final), es decir, la persona física que usa realmente los servicios de computación en nube en un contexto específico. El usuario puede coincidir con el abonado, como en el caso de Tim, pero también puede ser otra persona; Eleni es el usuario final del servicio de correo de Microsoft contratado por la Universidad de Tilburg.

Estas entidades pueden corresponderse con varios conceptos de la Directiva sobre Protección de Datos.

La Directiva 95/46/CE sobre protección de datos

La Directiva 95/46/CE sobre protección de datos, promulgada en 1995, tiene como objetivo facilitar el libre flujo de información, manteniendo un nivel aceptable de privacidad de las personas.[9] La DPD trata de encontrar un equilibrio entre intereses contrapuestos. Por un lado, hay un interés claro por la privacidad de las personas. Por otro lado, hay libertad de expresión e intereses comerciales por prestar servicios para los que los datos personales son esenciales. Las obligaciones para las distintas partes implicadas en el tratamiento de datos personales tienen que ser vistas por lo que respecta a estos dos objetivos de la Directiva, que pueden estar en conflicto.

La DPD establece una serie de principios básicos de privacidad que deben garantizarse cuando los que la Directiva llama «responsables del tratamiento de datos» recogen o procesan datos personales. Un concepto básico de la Directiva es «datos personales» que, según el artículo 2 (a), significa «toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.» En las relaciones comerciales con los consumidores, los datos directamente identificadores, como el nombre, y los datos indirectamente identificadores, como el número de teléfono u otros números, (por ejemplo, número de cliente y número de la seguridad social) son relevantes.

Por lo que respecta a la computación en nube, tenemos que evaluar si los datos que se usan en las situaciones de servicios de computación en nube son datos personales según la Directiva sobre Protección de Datos. Esta es la pregunta fácil. En muchos casos, se procesarán datos personales. Las tres situaciones descritas en la sección anterior implican grandes cantidades de datos personales.[10] Las direcciones electrónicas (del emisor y del receptor) son datos personales, lo mismo que el contenido que se refiere a personas identificables, pero también son datos personales, en general, las direcciones IP de los equipos usados en las diferentes situaciones y las *cookies* fijadas por los proveedores.[11]

Los titulares de los datos o interesados en los modelos de computación en nube pueden ser el usuario cuyos datos personales (como información de la cuenta, direcciones IP, *cookies*, direcciones electrónicas, preferencias, patro-

9. DPD 9 preámbulo artículo 3.
10. Véase también Catteddu y Hogben, 2009.
11. Véase, por ejemplo Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2007; Leenes, 2008a.

nes de uso, atributos) se procesan, pero también otros que se mencionan, o se refieren, en el contenido concreto tales como los comentarios o las etiquetas en los sitios de redes sociales, o las imágenes que retratan individuos identificables.[12]

El tratamiento de datos personales de acuerdo con el artículo 2 b de la Directiva sobre Protección de Datos, significará «cualquier operación o conjunto de operaciones, efectuadas o no, mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, uso, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los datos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.» De nuevo, no es difícil ver que muchos servicios de computación en nube procesan datos personales.

El responsable del tratamiento de datos

Los conceptos de *responsable del tratamiento de datos* y *encargado del tratamiento de datos* son más difíciles. Según el artículo 2 d de la Directiva, el «responsable del tratamiento» será «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el derecho nacional o comunitario.» Mientras que el apartado e de dicho artículo define el término *encargado del tratamiento* como la entidad que «trata datos personales por cuenta del responsable del tratamiento».

Qué entidad tiene que ser calificada como responsable del tratamiento es relevante por dos razones. En primer lugar, determina si la Directiva es aplicable en un caso particular (ley aplicable) y, en segundo lugar, determina quién tiene ciertas responsabilidades y obligaciones (asignación de responsabilidades).

La aplicabilidad de la DPD se determina en el artículo 4 de la Directiva, que establece:

> «1. Los estados miembros aplicarán las disposiciones nacionales que hayan aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:
>
> a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el derecho nacional aplicable;
>
> b) el responsable del tratamiento no esté establecido en el territorio del estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del derecho internacional público;
>
> c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho estado miembro, salvo en caso de que dichos medios se usen solo con fines de tránsito por el territorio de la Comunidad Europea.
>
> 2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.»

Esta disposición establece una distinción entre los responsables del tratamiento físicamente 1 (a) o legalmente 1 (b) ubicados en un estado miembro de la UE o, si se encuentran fuera de la UE, hacen uso de equipos para el tratamiento de datos personales (que no sea exclusivamente la transmisión de datos desde el territorio de la Comunidad a un tercer país, que excluye los routers etc.) 1 (c).

En los casos tradicionales, es decir, en la era anterior a Internet, esto ofrecía suficiente orientación. Por lo general, los equipos usados para el procesamiento de datos personales (ordenador central, miniordenador o PC) residían en el lugar de la entidad responsable del tratamiento (por ejemplo, un hospital o una sede de empresa), en cuyo caso es fácil determinar quién es el responsable del tratamiento. Sin embargo, hoy en día esto no es tan sencillo como en el caso de las situaciones de computación en nube. La Universidad de Tilburg usa los servicios de Microsoft. Microsoft tiene su sede principal en Redmond,

12. Véase por ejemplo Kuczerawy, 2010; Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2009.

Estados Unidos, pero también tiene oficinas en muchos países. Sus instalaciones de computación en nube también se encuentran en diferentes países y, posiblemente, en los mismos lugares que sus oficinas, pero es más probable que se encuentren en centros de datos en otros lugares. En situaciones de computación en nube más complejas, algunas terceras partes forman parte del entorno de servicio. Por ejemplo, en el caso de Facebook, existen agregadores de publicidad que participan, así como proveedores de aplicaciones para las aplicaciones que se ejecutan en el entorno de Facebook.

En otras palabras, la ubicación donde se toman las decisiones relativas a «los propósitos y los medios del tratamiento de datos personales» puede no coincidir con la ubicación donde se lleva a cabo el tratamiento real y puede haber varias entidades involucradas en la toma de decisiones con fines distintos, lo que significa que puede haber varios responsables del tratamiento (y encargados del tratamiento) en las diferentes situaciones de computación en nube.

Lo que determina quién es el responsable del tratamiento es: la ubicación de la entidad jurídica responsable de decidir sobre los «fines y medios» del tratamiento de datos personales o la ubicación del tratamiento real. Si la entidad jurídica es determinante, entonces, en el caso de la Universidad de Tilburg, no importa dónde se almacenen los datos de los estudiantes de Tilburg, siempre y cuando su parte contratante se encuentre en territorio de la Unión Europea (como es el caso: Microsoft Nederland), los datos de los estudiantes están protegidos por la DPD de la Unión Europea. No obstante, si la ubicación del tratamiento es determinante, entonces puede que sea importante dónde se tratan y almacenan los datos.[13]

El informe ENISA sobre las ventajas y riesgos de la computación en nube (Catteddu y Hogben, 2009, pág. 100) llega a la conclusión, basándose en el artículo 4 de la DPD, de que el lugar donde esté establecido el responsable del tratamiento es relevante para la aplicabilidad de la DPD[14] y que el lugar de tratamiento de datos personales y la residencia del interesado no son pertinentes a este respecto. Esto se corresponde con el dictamen del Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2002, pág. 6), que establece que la «directiva usa el criterio o "factor de conexión" del "lugar de establecimiento del responsable del tratamiento" o, en otras palabras, el principio del país de origen habitualmente aplicado en el mercado interior.»

Además, «el lugar, en el que se establece un responsable de tratamiento, implica el ejercicio efectivo y real de la actividad mediante una instalación estable y tiene que ser determinado en conformidad con la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. Según el Tribunal, el concepto de establecimiento implica el ejercicio efectivo de una actividad mediante un establecimiento fijo durante un período indefinido.[15] Este requisito también se cumple cuando una empresa se constituye para un período determinado.» Para dejar en claro que el Grupo de Trabajo no mezcla personalidad jurídica y ubicación de la tecnología, añade: «El lugar de establecimiento de una empresa que presta servicios mediante un sitio en Internet no es el lugar en que se encuentra la tecnología de apoyo a su sitio web o el lugar en el que su sitio web es accesible, sino el lugar donde se desarrolla la actividad.»[16]

El dictamen 169 del Grupo de Trabajo (2010) añade que «ser un responsable del tratamiento de datos es principalmente la consecuencia de la circunstancia real que una entidad ha escogido para tratar datos personales para sus propios fines» (pág. 8). En dicho dictamen, se hace una distinción entre el control derivado de la competencia legal explícita (por ejemplo, el nombramiento por legislación nacional), la competencia implícita (por ejemplo, los

13. Por el momento, dejo estar la aplicabilidad de las leyes extranjeras (no de la UE). Por ejemplo, si los datos se almacenan en el territorio de los Estados Unidos, se aplica la *USA Patriot Act*, que tiene consecuencias de largo alcance. Algunos contenidos que están permitidos por la legislación comunitaria, pueden no ser admisibles en los EE. UU., lo que significa que los ciudadanos de la UE podrían correr riesgos cuando sus datos se almacenen en los EE. UU.
14. Véase también Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2002, pág. 6, que establece que la «directiva usa el criterio o "factor de conexión" del "lugar de establecimiento del responsable del tratamiento" o, en otras palabras, el principio del país de origen habitualmente aplicado en el mercado interior.»
15. Caso C-221/89 Factortame [1991] ECR I-3905 §20.
16. Directiva 2000/31/CE, Considerando 19.

empresarios en relación a los datos de sus empleados), y el control que se deriva de la influencia fáctica (hechos del caso). La última categoría parece muy relevante en los casos de servicios de computación en nube.

El lugar de establecimiento del responsable del tratamiento como criterio de decisión, en vez de lugar de tratamiento, tiene sentido. La decisión de qué tratar y con qué fin es lo que más afecta a los interesados. Que el tratamiento real de estos datos con el fin de prestar un servicio particular en un momento determinado se podría hacer más eficiente o eficazmente en el punto X, mientras que mover todos los datos a la ubicación Y un poco después para lograr los mismos objetivos, en realidad no importa al interesado. ¿O sí le importa? Como el responsable del tratamiento de datos tiene la responsabilidad de tomar medidas de seguridad adecuadas, la ubicación real del tratamiento y almacenamiento afecta al titular de los datos, pero posiblemente en menor medida en condiciones normales.

Sin embargo, aquí no acaba todo.

En el caso en el que el responsable del tratamiento se encuentre fuera del territorio de la Unión Europea, no se puede aducir el factor de conexión «país de origen» para determinar cuál es la legislación aplicable. En ese caso, tal como está articulado en el artículo 4, apartado 1 letra c de la Directiva, la ubicación de los equipos de procesamiento es lo que cuenta. En otras palabras, si el responsable del tratamiento que reside fuera de la UE usa equipos para el tratamiento de datos personales situados en un estado miembro, entonces, la DPD sigue siendo válida y la legislación de ese estado miembro es la que regula el tratamiento de datos.

A menudo no es tan difícil establecer que un proveedor de servicios de computación en nube procesa datos personales y decide sobre los fines y los medios del tratamiento de datos personales, incluso en los casos de entidades que no residen en territorio de la Unión Europea. Facebook, con sede en Palo Alto, California, determina qué datos recoger de sus usuarios. Google, también con sede en California, determina qué datos personales procesar en el caso de Google Apps y Gmail. Pero, ¿usan estos proveedores de servicios de computación en nube los equipos en un estado miembro de la Unión Europea si una persona en el territorio de la Unión Europea recurre a sus servicios, que es el requisito para que la DPD sea aplicable a sus operaciones en la Unión Europea? Depende. Como se indica en el artículo 4, apartado 1 letra c, el equipo tiene que usarse para el tratamiento de datos personales, los meros instrumentos de transmisión están excluidos. Si el usuario solo usa el navegador para introducir datos en formularios de páginas web que ofrecen dichos responsables del tratamiento, la respuesta es no. El PC del usuario se usa entonces solamente para la transmisión, como los routers, interruptores y cables. Pero esto cambia cuando estos proveedores de servicios de computación en nube usan *cookies*, JavaScript, código Flash etc. El Grupo de Trabajo del Artículo 29, en su dictamen 56 (2002, págs. 10-11), por ejemplo, sostiene que «el PC del usuario es el equipo en el sentido del artículo 4, apartado 1 letra c de la Directiva 95/46/CE. Está ubicado en el territorio de un estado miembro. El responsable del tratamiento decidió usar este equipo para tratar datos personales, [...] El responsable del tratamiento dispone sobre el equipo del usuario y este equipo no se usa solo para fines de tránsito por el territorio de la Comunidad. El Grupo de Trabajo es por lo tanto de la opinión de que la ley nacional del estado miembro donde se encuentre el ordenador personal del usuario se aplica a la cuestión de en qué condiciones sus datos personales pueden ser recogidos mediante la colocación de cookies en su disco duro.»[17]

La última frase parece un contrasentido –recoger datos mediante la colocación de datos en el PC del usuario–, pero, de hecho, el proveedor de servicios usa la *cookie* para reconocer al usuario y ser capaz de rastrear su comportamiento a largo plazo. Aun así, equiparar las *cookies* con el equipo parece una idea descabellada. Puede que se trate de un problema de lenguaje;[18] las versiones anteriores de la Directiva usaban el término *medios*, que describe mejor lo que son las *cookies* que los equipos, que se refieren a las herramientas y dispositivos.

17. Esta opinión ha sido confirmada en el artículo 29 del dictamen del grupo de trabajo sobre los motores de búsqueda (artículo 29 Grupo de Trabajo sobre Protección de Datos, 2008) y el artículo. 29 del dictamen del grupo de trabajo sobre los sitios de redes sociales (artículo 29 Grupo de Trabajo sobre Protección de Datos, 2009).
18. Consulte la nota 22 en Grupo de Trabajo 56.

Sin embargo, las *cookies* plantean una cuestión más importante. Como ya se ha mencionado, si los proveedores de servicios de computación en nube no usasen *cookies* (ni JavaScript etc.) en sus servicios, entonces quedarían fuera de la jurisdicción de la DPD, mientras que si usan *cookies*, quedarían incluidos en el ámbito de aplicación de la DPD. Aleksandra Kuczerawy (2010, págs. 80-82) ofrece un interesante análisis de este asunto en el caso de los sitios de redes sociales. El artículo 5 (3) de la Directiva sobre privacidad y comunicaciones electrónicas 2002/58/CE establece que los proveedores de servicios solo pueden almacenar información o acceder a la información almacenada en el equipo de un abonado o usuario a condición de que el abonado o usuario en cuestión disponga de información clara y completa de conformidad con la Directiva 95/46/CE, entre otras cosas en particular sobre los fines del tratamiento, y cuando el responsable del tratamiento le ofrezca el derecho a rechazar ese tratamiento.

El fin de esta disposición es el de proteger a los ciudadanos europeos. Paradójicamente, si un usuario de la Unión Europea rechaza las cookies, la protección prevista por el artículo 4, apartado 1 letra c de la DPD desaparece.

Si un proveedor de servicios de computación en nube ubicado fuera del territorio de la Unión Europea que atiende a sus clientes dentro de la Unión Europea tiene que calificarse como responsable del tratamiento (por ejemplo, porque usa cookies), entonces tiene que cumplir con la normativa de protección de datos de cada uno de los estados miembros a los que ofrece servicios.[19]

La excepción de las actividades domésticas

La DPD contiene otra condición para la aplicación de la Directiva: la excepción de las actividades domésticas articulada en el artículo 3 apartado 2. «Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales: efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.» Esta condición es relevante por lo que respecta a los servicios de computación en nube usados por los individuos y en particular en el caso de las personas que usan sitios de redes sociales.

Ya en el 2003, el Tribunal de Justicia Europeo en el caso Lindqvist[20] decidió que «El acto de referir, en una página web, a diversas personas e identificarlas por su nombre o por otros medios, por ejemplo, su número de teléfono o información relativa a su condiciones de trabajo o a sus aficiones, constituye tratamiento de datos personales» y que «este tipo de tratamiento de datos personales no está cubierto por ninguna de las excepciones previstas en el artículo 3 apartado 2 de la Directiva 95/46.»

El Grupo de Trabajo del Artículo 29 de acuerdo con Lindqvist sostiene la opinión de que cuando los usuarios facilitan datos a un gran número de terceras partes, algunas de las cuales en realidad no conocen, podría ser una indicación de que la exención de las actividades domésticas no se sostiene y, por lo tanto, el usuario se consideraría un responsable del tratamiento de los datos. Si el usuario actúa en nombre de una empresa o asociación, la excepción de las actividades domésticas no se sostiene.

Consecuencias

Determinar el papel exacto de las partes implicadas es importante porque, como se ha dicho, determina las responsabilidades de estas partes con respecto al tratamiento de datos personales. La aplicabilidad de la normativa de protección de datos de la Unión Europea significa lo siguiente, entre otras cosas:

- El responsable del tratamiento debe definir claramente la finalidad del tratamiento como uno de los requisitos para permitir la recogida lícita y legal de los datos personales (artículo 6 de la DPD).
- El responsable del tratamiento debe garantizar que los datos sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben (artículo 6 de la DPD).
- La recogida de datos debe estar basada en un motivo legítimo (consentimiento inequívoco, cumplimiento de

19. Lo que se ha calificado como una «carga imposible» (Kuner, 2007).
20. C 101/01 (2003).

un contrato, cumplimiento de una obligación jurídica, en virtud de los intereses legítimos del responsable del tratamiento etc.) (artículo 7 de la DPD).

- El interesado tiene derecho de acceso y de rectificación o borrado de sus datos personales (artículo 12 de la DPD).
- El interesado, por lo menos, tiene que estar informado sobre la identidad del responsable del tratamiento y su representante, si lo hay, sobre la finalidad de la recogida, sobre los beneficiarios y sobre sus derechos (artículo 10 de la DPD).
- El responsable del tratamiento debe aplicar las medidas técnicas y organizativas adecuadas para proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, divulgación o acceso no autorizado, en particular cuando el tratamiento incluya la transmisión de datos a través de una red, y contra todas las otras formas ilegales de tratamiento (artículo 17 de la DPD).

¿Quién controla la nube?

Volvamos ahora a las situaciones de computación en nube descritas antes para calificar los diferentes actores a la vista de los conceptos expuestos en la sección anterior.

Resulta que en muchas situaciones de computación en nube hay una pluralidad de responsables del tratamiento y encargados del tratamiento que o bien tienen control conjunto o bien control secuencial. La misma entidad puede ser un responsable del tratamiento de datos para un fin y un encargado del tratamiento para otros fines. El abonado puede ser responsable del tratamiento, encargado del tratamiento de los datos o titular de los datos. El usuario final puede ser meramente el titular de los datos, pero, en algunos casos, el usuario final también puede calificarse como responsable del tratamiento.

En el caso de Eleni, por ejemplo, Microsoft no es solo un responsable del tratamiento de datos (en cuanto al tratamiento de los datos de la cuenta de Eleni y también si Microsoft usase los datos de Eleni para otros fines), sino que también lo es la Universidad de Tilburg, que puede calificarse como responsable del tratamiento, ya que pone los datos de Eleni en «manos» de Microsoft. Para las partes del tratamiento por las que la Universidad de Tilburg puede considerarse el responsable del tratamiento de los datos, Microsoft actúa como encargado del tratamiento.

En el caso de Tim, Facebook es un responsable del tratamiento de datos, pero, si Tim pone información sobre individuos identificables a disposición de un público lo suficientemente grande, también se convierte en responsable del tratamiento de esta información. Si la información solo es visible para su pequeño grupo de amigos, la excepción de actividades domésticas se aplica a sus acciones. El autor de este artículo puede ser un responsable del tratamiento de datos si trata datos de carácter personal siempre que elija los fines y los medios. La excepción de actividades domésticas no se aplica aquí, porque opera en nombre de su patrón. Si su patón, la Universidad de Tilburg, determina que tiene que usar Google Apps para fines específicos relativos a datos de carácter personal, por ejemplo, la calificación de trabajos cargados en Google Apps, entonces, la Universidad de Tilburg puede ser el responsable del tratamiento y Google se limita a ser el encargado del tratamiento.

Lo que estos ejemplos demuestran es que, en las situaciones de servicios de computación en nube, puede aparecer un paisaje muy difuso. A pesar de que la Directiva pretende garantizar «que, incluso en entornos complejos de procesamiento de datos, donde los diferentes responsables del tratamiento de datos desempeñan una función en el tratamiento de datos personales, el cumplimiento de las normas de protección de datos y las responsabilidades de posible incumplimiento de estas reglas están claramente asignadas, a fin de evitar que la protección de los datos personales se reduzca o que aparezca un "conflicto negativo de competencias" y surjan lagunas en las que algunas de las obligaciones o derechos derivados de la Directiva no estén garantizados por ninguna de las partes.» (Grupo de Trabajo sobre Protección de Datos del Artículo 29, 2010, pág. 22).

No estoy tan seguro de que las responsabilidades puedan asignarse claramente. En muchas situaciones de servicios (públicos) de computación en nube, donde los usuarios tienen cuentas, se usan *cookies* y *scripts* en línea, el servicio incorpora la funcionalidad de otras empresas (por ejemplo, las aplicaciones que se ofrecen en Facebook) y servicios (por ejemplo, los anuncios que ofrece otra empresa), y el usuario revela información sobre otras personas, la complejidad puede ser significativa y las entidades intentarán descargar sus responsabilidades a otras personas.

Pero incluso si la responsabilidad se pudiera asignar con claridad, ¿cuál sería su importancia práctica? ¿Supondría un nivel adecuado de protección de los ciudadanos de la Unión Europea? ¿Qué significa que el usuario final se califique como responsable del tratamiento de datos? ¿Cómo, por ejemplo, va el usuario final a cumplir con las medidas de seguridad que le impone el artículo 17 de la DPD en tal caso? O ¿cómo puede cumplir con el requisito de limitación de la finalidad impuesta por el artículo 6 de la DPD?

¿Cuánto control tiene un usuario final en situaciones en las que existen regímenes tipo «lo tomas o lo dejas», como suele suceder en los servicios públicos de computación en nube? Los usuarios finales tienen una posición negociadora muy débil frente a los grandes proveedores de servicios de computación en nube como Google, Facebook y Microsoft.[21]

Los abonados, sobre todo en el caso de que sean personas jurídicas, pueden tratar de negociar las condiciones que les permitan cumplir sus propias obligaciones, pero incluso en ese caso hay un desequilibrio de poder entre los proveedores de servicios de computación en nube (generalmente grandes) y los clientes, más débiles (Véase, por ejemplo Catteddu y Hogben, 2009, págs. 97-98).

La pregunta fundamental es si la computación en nube, con su pluralidad de entidades participantes y la fluidez de los datos y del tratamiento señala una clara necesidad de reconsiderar los conceptos y funciones básicas de la Directiva de Protección de Datos. ¿Tiene la «territorialidad» de las normas de protección de datos que ser definida de distinta manera en función de las tareas (por ejemplo, seguridad o transparencia) y los actores (responsable del tratamiento o encargado del tratamiento de datos)? y, si es así, ¿cómo? (Poullet y otros, en prensa).

Conclusión

En este artículo, he expuesto una visión de algunas de las cuestiones básicas de protección de datos que plantea la computación en nube. La distinción clara entre los controladores de datos y sus ayudantes, los encargados del tratamiento, por un lado, y los interesados, por el otro, ya no es un modelo adecuado del tratamiento de datos personales. Tampoco lo es la idea de que los datos se procesen para un conjunto único o limitado de propósitos. Los datos que se divulgan a las amistades también se usan para publicidad dirigida, servicios a medida etc. Esto hace opaco el vínculo entre los propósitos y los responsables del tratamiento (a pesar de que, al menos en teoría, los vínculos se puedan articular). La territorialidad de los responsables del tratamiento de datos también pierde su significado cuando los datos se trasladan de un centro de datos a otro y la mayoría de las veces esto no tiene importancia por lo que se refiere a la protección de la privacidad. Lo que importa es quién decide lo que ocurre con los datos. La forma actual de hacer que entidades de fuera de la Unión Europea pasen a estar bajo la jurisdicción de la Unión Europea (la ruta de las *cookies* en el equipo) me parece una solución enrevesada para hacer que los responsables del tratamiento de datos de fuera de la Unión Europea sean responsables de sus acciones. Y, por último, creo que fenómenos, tales como la web 2.0 y la computación en nube, dejan claro que todo el concepto de datos personales y lo que se pretende contribuir a facilitar y proteger requiere reflexión. Por supuesto, esto es precisamente lo que la Comisión está haciendo en vista de la revisión de la DPD.

Bibliografía

CATTEDDU, Daniele; HOGBEN, Giles (eds.) (2009). *Cloud Computing. Benefits, risks and recommendations for information security*. Heraklion: ENISA.

Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2002). Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento

21. E incluso el Grupo Trabajo del Artículo 29 parece tener solo una influencia limitada en empresas como Google y Facebook, a juzgar por la adopción laxa de las demandas del Grupo Trabajo del Artículo 29 por parte de estas empresas.

de los datos personales en Internet por sitios web establecidos fuera de la UE (WP 56). Aprobado el 30 de mayo de 2002.

Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2007). Dictamen 4/2007 sobre el concepto de datos personales (WP 136). Adoptado el 20 de junio de 2007.

Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2008). Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda (WP 148). Emitido el 4 de abril de 2008.

Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2009). Dictamen 5/2009 sobre las redes sociales en línea (WP 163). Adoptado el 12 de junio de 2009.

Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2010).Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (WP 169). Adoptado el 16 de febrero de 2010.

KUCZERAWY, Aleksandra (2010). «Facebook and Its EU Users – Applicability of the EU Data Protection Law to US Based SNS». En: M. BEZZI *et al.* (eds.). *Privacy and Identity Management for Life*. IFIP Advances in Information and Communication Technology. Boston: Springer. Pág. 75-85.

LEENES, Ronald (2008a). «Do They Know Me? Deconstructing Identifiability». *University of Ottawa Law & Technology Journal*. Vol. 4, n.º 1 y 2, pág. 135-61.

LEENES, Ronald (2008b). Protecting identity online: law and technology? – User-centric identity management as an indispensable tool for privacy protection. *International Journal of Intellectual Property Management*. Vol. 2, n.º 4, pág. 345-371.

MEIL, P.; GRANCE, T. (2009). Definición de *Cloud Computing* del NIST. Versión 15, 10-07-09. Gaithersburg, MD: National Institute of Standards and Technology (NIST). <http://csrc.nist.gov/groups/SNS/cloud-computing/>

POULLET, Yves; VAN GYSEGHEM, Jean-Marc; MOINY, Jean-Phillipe; GÉRARD, Jacques; GAYREL, Claire (en prensa, 2011). «Data protection in the clouds». En: Serge GUTWIRTH; Yves POULLET; Paul DE HERT; Ronald LEENES (eds.). *Computers, Privacy and Data Protection. An Element of Choice*. Dordrecht: Springer.

VAN GYSEGHEM, Jean-Marc; GÉRARD, Jacques; GAYREL, Claire; MOINY, Jean-Phillipe; POULLET, Yves (2010). *Cloud computing and its implications on data protection*. Namur: CRID. <http://www.crid.be/pdf/public/6471.pdf>

Cita recomendada

LEENES, Ronald (2010). «¿Quién controla la nube?». En: «VI Congreso Internet, Derecho y Política. *Cloud Computing*: El Derecho y la Política suben a la Nube» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 11. UOC. [Fecha de consulta: dd/mm/aa].

<http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-leenes/n11-leenes-esp>

ISSN 1699-8154

Sobre el autor

Ronald Leenes
r.e.leenes@uvt.nl

El Dr. Ronald Leenes es catedrático de Regulación mediante Tecnología en el TILT, el Instituto de Derecho, Tecnología y Sociedad de Tilburg (Universidad de Tilburg). Sus principales campos de estudio son la gestión de la privacidad y la identidad, y la regulación de la tecnología y con la tecnología. Además, está implicado en estudios de fraude de identidad, biometría y resolución de conflictos por Internet.

Tilburg Institute for Law, Technology, and Society
Tilburg University
Warandelaan 2
5037 AB Tilburg, Países Bajos