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

David Martínez (coord.)

Sumario

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

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

Cloud computing y protección de datos

Ramón Miralles

Fecha de presentación: octubre de 2010
Fecha de aceptación: octubre de 2010
Fecha de publicación: diciembre 2010

Resumen

El *cloud computing* es una arquitectura de prestación y/o aprovisionamiento de servicios de tecnologías de la información y la comunicación, que está tomando mucho protagonismo, y que, según los analistas, en los próximos años se consolidará tanto por lo que respecta a los usuarios individuales de la red y servicios en línea, como en las empresas, que afectará a su manera de utilizar las TIC.

Con relación a los usuarios de la red el *cloud computing* tiene muchos puntos de conexión con la Web 2.0 y para las empresas está estrechamente relacionado con los procesos de *outsourcing* de los servicios TIC.

En este artículo se identifican y analizan las cuestiones más relevantes del binomio *cloud computing* y protección de datos de carácter personal.

Palabras clave

cloud computing; protección de datos, libertades, privacidad, informática en nube, encargado tratamiento, transferencias internacionales

Tema

Derecho fundamental, protección de datos, sociedad de la información

Cloud computing and data protection

Abstract

Cloud computing is an architecture for carrying out and/or providing services for information and communication technologies which is playing an increasingly prominent role. According to analysts, among companies and individual users of the Internet and online services, its application will be consolidated over the next few years.

In relation to Internet users, cloud computing has many connections with the web 2.0, and for companies it is closely linked to outsourcing of ICT services.

This article identifies and analyses the major questions regarding binomial cloud computing and private data protection.

Keywords
cloud computing, data protection, freedom, privacy, data processing requests, international transferences

Topic
Basic rights, Data protection, Information society

El *cloud computing* es una arquitectura de prestación y/o aprovisionamiento de servicios de tecnologías de la información y la comunicación que, en los últimos dos años, está adquiriendo bastante protagonismo. Según los analistas, en los próximos años se consolidará tanto entre los usuarios particulares de la red y servicios en línea, como entre las empresas; en ambos casos afectará a su manera de utilizar las TIC.

Respecto a los usuarios de la Red, la informática de nube tiene muchos puntos de conexión con la web 2.0 y, en el caso de las empresas, está estrechamente relacionada con los procesos de externalización de los servicios TIC.

Mi primer contacto profesional con el concepto *cloud computing* fue mediante un documento de mayo del 2008, concretamente un *white paper* de la oficina del Comisariado de Información y Privacidad de Ontario (Canadá), cuyo título es «Privacy in the clouds».[1]

El documento en sí mismo no aporta, en estos momentos, una reflexión relevante en cuanto a la protección de datos personales y el *cloud computing*, dado que tiene un carácter muy introductorio y se dedica fundamentalmente a la identidad digital en Internet. Por lo tanto, no aborda en profundidad ni de manera amplia la privacidad en relación con el *cloud computing*, pero a mí me sirvió para tomar contacto con este nuevo concepto.

Existe otro documento, también del IPC de Ontario, que sí aborda con más detalle la cuestión de la privacidad y el *cloud computing*. Lleva por título *Modeling Cloud Computing Architecture Without Compromising Privacy*: *A Privacy by Design Approach* y se publicó en mayo del 2010; ambos se pueden descargar en la página web del IPC.

El primero de los documentos a los que he hecho referencia sí que pone énfasis, en su introducción, al hecho de que la autodeterminación informativa es un concepto que ha ser promovido y protegido en un contexto en el que importantes cantidades de información de carácter personal (el documento habla de cantidades «ilimitadas») pasan de los individuos a las organizaciones, y de éstas a otras organizaciones. Y yo añadiría que este rasgo ilimitado no hace referencia exclusivamente a la cantidad de información, sino al tipo y a los formatos de la información.

Después volveré a referirme a la autodeterminación informativa, que como veremos está especialmente afectada por las características de procesamiento de la información del *cloud computing*.

Ahora querría continuar, en clave introductoria, con una breve referencia al origen del *cloud computing*. Desde la óptica de las telecomunicaciones, se entiende por *cloud* o nube el conjunto de dispositivos e infraestructuras de comunicaciones por los que, de manera «impredecible», pasa la información cuando se quiere transmitir de un punto a otro de Internet. Esta falta de predicción afecta tanto al número como al tipo de dispositivos; de hecho, todos los elementos que se encuentran en medio de este intercambio de informaciones se han representado, tradicionalmente, como una nube.

1. La comisaria de Información y Privacidad de Ontario (IPC, Information and Privacy Commissioner, http://www.ipc.on.ca) es Ann Cavoukian, quien ha ocupado diferentes cargos en este comisariado desde el año 1987; a lo largo de su carrera profesional, ha destacado por prestar una atención especial a los aspectos tanto tecnológicos como organizativos de la protección de datos, al considerar que la tecnología tiene un papel clave en la protección de la privacidad. Por ello, ha promovido y ha participado en un buen número de publicaciones en las que se tratan cuestiones tecnológicas relacionadas con la privacidad y la protección de datos. Por ejemplo, es bastante conocida por haber trabajado conceptos como los de *privacy by design* y *privacy enhancement technologies* (PET).

El origen de la comunicación es conocido (un usuario o proceso inicia una transacción) y el de destino también (un servidor da respuesta a la transacción), y así sucesivamente. Pero el camino que seguirá la información transportada entre los dos puntos responde a unas reglas que, si bien están fijadas por un protocolo técnico (TCP), tienen resultados impredecibles a priori; de este modo, en la práctica podemos intuir por dónde pasará la información, pero sin estar del todo seguros.

Hay que añadir otro elemento, que es que a pesar de que en esencia estos dispositivos se dedican a gestionar el tránsito de la información entre origen y destino, no se nos puede escapar que durante este tránsito la información se puede someter a tratamientos que vayan más allá de facilitar la transmisión de paquetes de información.

Quiero recordar que existe un debate abierto respecto al uso de tecnologías de inspección de paquetes (*deep packet inspection*, DPI). Es decir, la capacidad que tienen algunos equipamientos de red, que no son punto final de comunicaciones, de tratar las cabeceras de los paquetes que debe retransmitir por la Red y, convenientemente configurado, de analizar su contenido.

De hecho, la circunstancia de que los datos personales se puedan tratar exclusivamente a efectos de tránsito por la Red está prevista en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales (LOPD). En cuanto a la determinación del ámbito territorial de aplicación, el art. 2.1.a prevé que la LOPD es aplicable cuando el responsable del tratamiento, a pesar de no estar establecido en el territorio de la Unión Europea, utilice medios situados en el territorio español, excepto si estos medios se utilizan únicamente con el fin de tránsito.

Ahora bien, en el momento en el que la nube deja de ser exclusivamente un medio de transporte de la información, para pasar a tener capacidad de procesamiento de la información, se le añade el *computing*; a pesar de que en realidad la capacidad de procesamiento no recae exactamente en la nube, sino en aplicaciones, plataformas e infraestructuras disponibles en la Red y de que, en algunos aspectos, se comportan como los dispositivos de la nube a la que he hecho referencia.

El *cloud computing* implica que en el procesamiento de información concurre una serie de características cuya consecuencia directa es que el origen, y especialmente el destino, de una transacción deja de tener unos valores absolutos para pasar a tener otros relativos: la información no siempre se halla donde realmente parece y no siempre es tratada donde parece que se está procesando.

La definición de *cloud computing* que generalmente sirve de base para dotar de contenido a este concepto es la del NIST[www1] (Instituto Nacional de Estándares y Tecnologías, una agencia del US Department of Commerce, creada en 1901). La última versión de esta definición de *cloud computing* elaborada por el NIST es de julio del 2009.

Según esta definición, hay 5 características que definen el *cloud computing*:

- Autoservicio: el usuario puede utilizar más capacidades de procesamiento o almacenamiento de la información, sin pedirlo expresamente al proveedor del servicio.
- Amplio acceso a la Red: se puede acceder a ésta desde diferentes dispositivos y redes.
- Agrupación y reserva de recursos: hay un conjunto de recursos compartidos por los usuarios, de acuerdo con sus necesidades puntuales, que implica que en cada momento los recursos reservados puedan ser diferentes.
- Rapidez y elasticidad: se puede acceder a los nuevos recursos de manera inmediata y aparentemente ilimitada.
- Servicio medible y supervisado: se controla el uso y en todo momento se puede conocer, de manera transparente, el nivel de recursos utilizado.

Esta capacidad de proceso en la nube está conectada con la tendencia de externalización de los servicios TIC de las organizaciones y la reconversión de estos servicios al denominado *utility computing*.

Respecto a esta cuestión, recomiendo la lectura del artículo de Nicholas Carr[2] publicado en la *MIT Sloan Manage-*

2. Nicholas Carr es autor del *best seller* del 2008 del *Wall Street Journal, El gran cambio: cableando el mundo, desde Edison a Google*, considerado uno de los libros más influyentes en el *cloud computing*. (http://www.nicholasgcarr.com/info.shtml)

[www1] http://www.nist.gov

ment Review (Massachusetts Institute of Technology), de abril del 2005, que con el título «The End of Corporate Computing»[www2] describe los motivos que deben llevar a las organizaciones a dejar de considerar las TIC como un activo de su propiedad, para pasar a tratarlas como un servicio que compran.

En su artículo, Carr hace un paralelismo entre el proceso de transformación del uso de las TIC que deben seguir las organizaciones para ser competitivas con la transformación que se produjo a principios del siglo XX, cuando las empresas industriales empezaron a cerrar y a desmantelar las fuentes de energía utilizadas por sus industrias y que eran de su propiedad (molinos de agua, máquinas de vapor, generadores eléctricos, etc.).

Aproximadamente a partir de 1880, la producción comercial de electricidad empezó a ser posible; en 1902, en Estados Unidos había unas 50.000 plantas de generación privada de energía y sólo 3.600 estaciones podían vender energía a otras, con muchas limitaciones e inicialmente con un precio alto. Pero entre 1907 y 1920 la cuota de producción de energía eléctrica para ser comercializada pasó del 40 al 70%, y en 1930 ya alcanzaba el 80%.

Los motivos de esta rápida adopción de un nuevo modelo de suministro de energía para las industrias eran sencillos: unos costes menores y una complejidad de gestión menor, que permitía que las industrias se pudieran centrar en su negocio.

Para Nicholas Carr, en su artículo del 2005, existen tres avances tecnológicos clave en la transformación de las TIC: la virtualización, el *grid computing* y los servicios web, que, combinados con el aumento de capacidad de las redes de comunicaciones y la fibra óptica, dan como resultado un escenario idóneo para llevar a cabo esta transformación, de modo que el mayor obstáculo no será la tecnología, sino la actitud de las organizaciones a la hora de asumir este nuevo modelo de uso de las TIC en sus negocios.

Lo cierto es que el *cloud computing* ya es una realidad para los usuarios de la Red, a título individual. Los principales casos de uso del *cloud computing* implican compañías y servicios como Facebook, Amazon, Nasdaq o Google. En un informe del Pew Research Center,[3] de septiembre del 2008, se señalaba, con relación al uso del *cloud computing*, que el 69% de los usuarios de Internet de Estados Unidos almacena datos o utiliza aplicaciones basadas en servicios de *cloud computing*.

La explosión real del *cloud computing* vendrá provocada por este modelo de uso de las TIC por parte de las empresas.[4] Tal y como el propio NIST incluye en su definición, el *cloud computing* es un paradigma que todavía está en evolución.

Llegados a este punto, ya podemos empezar a hablar de algunos elementos clave a la hora de hablar de *cloud computing* y la protección de datos: la obtención de servicios TIC prestados por terceros, especializados en el procesamiento de información, y lo que en el contexto de la protección de datos conocemos como el encargado del tratamiento.

También podemos avanzar un segundo elemento de relevancia, que –aunque no siempre estará presente– si es consecuente con el paradigma del *cloud computing* y lo que éste implica como ahorro de costes, tendrá mucho peso. Este segundo elemento será la prestación de estos servicios por parte de empresas globales, ubicadas en aquellos lugares del mundo en los que la instalación de centros de proceso de datos orientados al *cloud computing* resulte más rentable. A menudo, esto implicará la aplicación de la figura del movimiento internacional de datos personales, también prevista en la normativa en materia de protección de datos de carácter personal.

Más adelante volveré a analizar con algo más de detalle estas dos cuestiones, pero ahora querría añadir algunos otros comentarios de carácter general.

3. http://pewresearch.org/. Un reciente informe de este centro de investigación (junio del 2010) recoge la opinión de los expertos de que en el 2020 la mayoría de los usuarios de Internet utilizará aplicaciones basadas en *cloud computing*, en lugar de las aplicaciones de escritorio (http://pewinternet.org/reports/2010/the-future-of-cloud-computing.aspx).
4. En este sentido, resulta de especial interés la tarea de Salesforce, con relación al uso empresarial del *cloud computing*. Ver http://www.salesforce.com/es/cloudcomputing/ y http://www.youtube.com/watch?v=VOn6tg3e1t4

[www2] http://sloanreview.mit.edu/the-magazine/articles/2005/spring/46313/the-end-of-corporate-computing/.

A pesar de que tanto la Directiva 95/46/CE, relativa a la protección de las personas físicas en cuanto al tratamiento de datos personales y a la libre circulación de estos datos, como la Ley Orgánica de Protección de Datos prevén estas dos circunstancias (encargadas del tratamiento y movimiento internacional de datos), su planteamiento con relación al tratamiento de la información es «preInternet»; es decir, un escenario de bases de datos centralizadas, tanto física como lógicamente (hardware y software), y situadas en centros corporativos de procesamiento de datos instalados en los locales de la organización responsable del tratamiento.

De hecho, las propias autoridades de control europeas reconocen que, a pesar de que las previsiones de la Directiva 95/46/CE se hicieron de una manera tecnológicamente neutra, y que parece que desde el año 1995 han ido resistiendo la continua evolución de las tecnologías y las redes, hay complejidades aportadas por esta evolución que generan cierta incertidumbre en cuanto a la asignación de responsabilidades en el tratamiento de los datos de carácter personal y en cuanto al alcance de las legislaciones nacionales aplicables.

No debemos olvidar que en el contexto de la protección de datos personales resulta esencial la identificación del responsable del tratamiento, dado que esto garantiza que hay una persona que tiene asignadas una serie de obligaciones concretas derivadas del tratamiento y, por lo tanto, hay alguien a quien se le puede exigir el cumplimiento de estas obligaciones.

Muchos de los servicios en línea que han emergido como consecuencia del uso intensivo y masivo de la Red en los últimos años han llevado al límite la legislación europea en materia de protección de datos; en algún caso, incluso ha resultado insuficiente para dar respuesta a las nuevas situaciones que surgen en Internet. De aquí que el grupo de autoridades de control que crea el art. 29 de la Directiva (conocido como grupo del art. 29) haya tenido que ir analizando y dictaminando sobre determinadas cuestiones.[5] De hecho, en el programa de trabajo 2010-2011 del grupo del art. 29 se incluye explícitamente analizar el *cloud computing* con relación a la protección de datos de carácter personal.

En el ámbito internacional, y por lo tanto más allá del contexto europeo, las autoridades de control de privacidad y protección de datos también han mostrado su preocupación por estas cuestiones. Resulta de especial relevancia la propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad, respecto al tratamiento de datos de carácter personal, acogida por la 31.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (5 de noviembre del 2009, Madrid). Esta propuesta es el resultado de una resolución previa de la 30.ª conferencia, que planteaba la necesidad urgente de proteger la privacidad en un mundo sin fronteras y de lograr una propuesta conjunta para el establecimiento de unos estándares internacionales sobre privacidad y protección de datos personales.

Los diferentes modelos de servicio de *cloud computing*, ya sea como servicio de software (SaaS), de plataforma (PaaS) o de infraestructura (IaaS), impactan directamente sobre una cuestión clave en la definición del derecho a la protección de datos de carácter fundamental: la autodeterminación informativa.

A pesar de que en función del modelo de despliegue del *cloud* el impacto es mayor o menor: nube pública, privada, híbrida (dos o más nubes diferentes) o comunitario.

Esta autodeterminación informativa, tal y como la definieron las sentencias 290/2000 y 292/2000 del Tribunal Constitucional, de 30 de noviembre del 2000, implica:

5. El «Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos en el tratamiento de los datos personales en Internet para lugares web ubicados fuera de la Unión Europea», aprobado el 30 de mayo del 2002; el «Dictamen 1/2008, sobre cuestiones de protección de datos relacionados con los motores de búsqueda»; el más reciente «Dictamen 5/2009, sobre las redes sociales en línea»; o el de principios de este año, «Dictamen 1/2010, sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento"», son algunos ejemplos relevantes. En este último documento se hace una referencia directa al *cloud computing* y a las dificultades que puede implicar para esta asignación de responsabilidades en materia de protección de datos. En http://ec.europa.eu/justice_hombre/fsj/privacy/workinggroup/wpdocs/ se pueden encontrar todos los documentos aprobados por el grupo del art. 29.

- En primer lugar, que «el derecho a la autodeterminación informativa es un derecho activo de control sobre el conjunto de informaciones relativas a una persona».
- En segundo lugar, que «el derecho a la protección de datos garantiza a los individuos un poder de disposición sobre» sus datos personales.
- Y en tercer lugar, que este poder de disposición sobre los propios datos personales no vale nada si el afectado desconoce qué datos de él tienen en su poder terceros, quién son estos terceros y con qué finalidad tienen sus datos.

Y éste es uno de los primeros inconvenientes detectados con relación al *cloud computing*: la pérdida efectiva de control sobre los datos, dado que más allá de los vínculos contractuales o de suscripción con las empresas que prestan estos servicios desaparece o «se nubla» el vínculo o la certeza sobre la ubicación física de la información y las condiciones de procesamiento y, en consecuencia, pueden quedar afectadas las garantías de confidencialidad y de seguridad de la información situada en el *cloud*.

Además, ésta no es una preocupación expresada únicamente por las autoridades de control; tal y como recoge un documento del NIST, de julio del 2009, «Effectively and Securely Using the Cloud Computing Paradigm» («Uso eficaz y seguro del *cloud computing*»), uno de los retos del *cloud computing* es la seguridad, a pesar de que el propio documento valora que «cloud security is a tractable problem».

En la misma línea, un estudio más reciente, de junio de este año, también de IDC, pero mucho más cercano porque se realizó con grandes empresas y organizaciones en Cataluña, evidencia que uno de los inhibidores de las empresas para dar el salto a la nube es la preocupación por la falta de confidencialidad de los datos (con una puntuación de 4,4 sobre 5, y a mucha distancia del resto de inhibidores).

Por último, un documento de la Cloud Security Alliance[6] (CSA), «Top Threats to Cloud Computing v1.0», de marzo del 2010, identifica las 7 principales amenazas que pueden afectar el despliegue del *cloud computing*, entre las que incluye la pérdida o fuga de datos (*data loss or leakage*).

Que la seguridad en el *cloud computing* es una cuestión de la que hay que ocuparse lo evidencian los recientes estudios, más o menos detallados, sobre ésta de distintas organizaciones. Aparte de algunos ya mencionados, podemos destacar los siguientes:

- «Privacy in the clouds: Risks to Privacy and Confidentiality from cloud computing», del World Privacy Forum[www3] (febrero del 2009)
- «Cloud computing. Information Assurance Framework» y «Cloud computing. Benefits, risks and recommendations for information security», de ENISA[www4] (ambos de noviembre del 2009)
- «Guía para la seguridad en áreas críticas de atención en *cloud computing*», de la CSA[www5] (también de noviembre del 2009)
- «Modeling cloud computing architecture without compromising privacy: a privacy by design approach», del Information and Privacy Commissioner de Ontario[www6] (mayo del 2010).

Antes de concluir esta parte introductoria, me gustaría evidenciar otros riesgos, derivados también de esta pérdida de control, que tienen que ver con el uso de los datos personales con fines de seguridad pública, dado que sin duda el *cloud computing* también puede convertirse en una oportunidad para que los cuerpos y fuerzas de seguridad puedan ejercer un mayor control sobre la población, y proteger así a la ciudadanía de actos violentos vinculados a la seguridad pública y a la seguridad de los estados.

Recomiendo consultar la web «Statewatch»[www7] (observatorio de la actividad de los estados y de las libertades

6. La Cloud Security Alliance tiene por finalidad promover el uso de las mejores prácticas en seguridad en el contexto del *cloud computing*, organización de la que, por cierto, recientemente se ha creado el capítulo español, uno de los primeros a nivel mundial. Se puede consultar en http://www.cloudsecurityalliance.org/.

[www3]http://www.worldprivacyforum.org
[www4] http://www.enisa.europa.eu
[www5] http://www.cloudsecurityalliance.org/
[www6] http://www.ipc.on.ca
[www7] http://www.statewatch.org

civiles en Europa) y la lectura del documento del Consejo de la Unión Europea, de abril del 2010, sobre el uso de un «instrumento estandarizado, multidimensional y semiestructurado de recogida de datos e información relacionada con los procesos de radicalización en la Unión Europea» (ENFOPOL 99), cuyo objeto es «evitar que las personas se conviertan en terroristas, abordando factores y causas profundas que puedan conducir a la radicalización y el reclutamiento tanto dentro como fuera de Europa».

Y es que no debemos olvidar que el derecho a la protección de datos personales tiene un carácter instrumental para el ejercicio otros derechos fundamentales y está íntimamente relacionado con las libertades públicas e individuales. Por lo tanto, se ha de tener presente que cuando hablamos de proteger los datos personales o de autodeterminación informativa estamos hablando, en definitiva, de libertad.

Respecto a los aspectos prácticos y más técnicos de la regulación en materia de protección de datos que, en relación con el *cloud computing*, hay que tener en cuenta desde una perspectiva de cumplimiento legal, ya he avanzado la primera cuestión que se debe analizar: incluso en la modalidad de despliegue privado del *cloud computing*, si la infraestructura de la nube es gestionada por un tercero, nos encontraremos con el supuesto de un «tratamiento por cuenta de terceros», es decir, con la figura de encargado de tratamiento, una situación regulada en el art. 12 de la LOPD.

Esto, sin entrar a discutir sobre las dificultades que en algunos casos se pueden dar en la determinación de quién es el responsable de un tratamiento, dado que ciertas situaciones no evidencian tanto la asignación de esta responsabilidad. En el contexto de la Directiva Europea, tiene que ver con aquella persona física o jurídica que determina las finalidades y los medios de tratamiento de los datos personales.

El dictamen 1/2010 del grupo del art. 29, al que ya he hecho referencia,[7] aborda esta cuestión con detalle y con ejemplos relacionados directamente con el *cloud computing*; en definitiva, se considera que, para la determinación del responsable del tratamiento, no sólo se hay que tener en cuenta las relaciones jurídicas, sino también las situaciones fácticas, de modo que se deben analizar las circunstancias de cada caso para asignar la responsabilidad sobre el tratamiento.

Antes de continuar con el encargado del tratamiento, hay una cuestión que querría tratar brevemente, en concreto sobre el ámbito de aplicación de la LOPD: en qué momento son de aplicación los requisitos y las condiciones del art. 12 de la LOPD, que regula la figura del encargado del tratamiento, para un tratamiento por cuenta de un tercero.

El ámbito de aplicación de la LOPD viene regulado en el art. 2, que prevé que la LOPD es de aplicación cuando:

- El tratamiento se efectúa en territorio español, en un establecimiento del responsable del tratamiento; aquí la territorialidad tiene un peso específico importante, que en el caso del *cloud computing* puede plantear serias dudas en cuanto a su verificación; como decíamos, estamos ante una óptica clásica de lo que son los centros de procesamiento de datos.
- El responsable del tratamiento no tiene un establecimiento en territorio español, pero en aplicación de las normas de derecho internacional público le es aplicable la normativa española.
- El responsable del tratamiento no está establecido en el territorio de la Unión Europea, pero utiliza medios de tratamiento situados en territorio español (con la excepción de que sólo sea con el fin de tránsito). Como resultado de la tarea interpretativa del grupo del art. 29, por ejemplo, el uso de galletas (cookies) se considera un uso de medios situados en el territorio del ordenador del usuario en el que se instalan las galletas (ver WP56, sobre la aplicación internacional de la legislación comunitaria de protección de datos).

El art. 3 del reglamento de despliegue de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), aporta algunos elementos adicionales con relación al ámbito territorial de aplicación del reglamento, que añade tres cuestiones que conviene comentar:

7. Ver nota 5.

1) Si el responsable del tratamiento no tiene un establecimiento en territorio español, pero tiene un encargado del tratamiento ubicado en España, le es de aplicación el título VIII del reglamento, es decir, las medidas de seguridad.
2) Si el responsable del tratamiento no está establecido en el territorio de la Unión Europea, pero utiliza medios situados en territorio español, este responsable del tratamiento debe designar un representante establecido en territorio español.
3) Y por establecimiento hay que entender cualquier instalación que permita el ejercicio efectivo y real de una actividad, con independencia de la forma jurídica adoptada.

Continuando con el tratamiento por cuenta de terceros, a fin de que la figura de encargado de tratamiento entre en juego y de que, por lo tanto, se considere que no hay una comunicación de datos, debe existir necesariamente una relación jurídica que vincule al responsable y al encargado de tratamiento y que delimite, de manera precisa, cuál será su actividad con relación al tratamiento de datos personales que realiza el encargado por cuenta del responsable del tratamiento.

En situaciones en las que un tercero preste servicios de *cloud computing,* diferente por lo tanto del responsable del tratamiento, y sea de aplicación la LOPD, hay que aplicar en toda su extensión lo previsto en el capítulo III del RLOPD (arts. 20, 21 y 22).

Una de las obligaciones que establece el RLOPD en el art. 20.2 es que el responsable del tratamiento debe velar por que el encargado del tratamiento cumpla con lo que prevé el reglamento. Por lo tanto, hay que articular estos mecanismos de supervisión, que en ciertas circunstancias serán de difícil implementación, especialmente cuando el encargado del tratamiento pueda tener una posición dominante en el mercado.

Otra cuestión de interés, que regula el art. 21, es la subcontratación de servicios, que parte del principio general de que el encargado del tratamiento no puede subcontratar a un tercero ningún tratamiento que le haya sido encomendado por el responsable del tratamiento. Ahora bien, sí que lo puede hacer si obtiene autorización del responsable del tratamiento, y siempre y cuando esta subcontratación la haga en nombre y por cuenta del responsable del tratamiento.

Hay algunas condiciones que permiten exceptuar la autorización del responsable del tratamiento:

- que esté ya especificado en el contrato de servicios que regula el encargo y que se indique la empresa que se subcontratará; y si no es posible esta determinación a priori, el encargado debe comunicar al responsable qué empresa piensa subcontratar antes de proceder a su subcontratación;
- que, obviamente, el subcontratista se ajuste a las instrucciones del responsable del tratamiento, ya dadas al encargado de éste, y
- que el encargado y el subcontratista formalicen un contrato; entonces el subcontratista tendrá la consideración de encargado de tratamiento.

Una vez finalizada la prestación contractual, también será de aplicación el régimen previsto con relación a la conservación de datos por parte del encargado del tratamiento; como regla general, los datos se deben destruir o devolver al responsable, excepto que alguna previsión legal obligue al encargado del tratamiento a conservar los datos. Eso sí, los datos deben estar bloqueados, es decir, no se pueden someter a ningún tipo de tratamiento que vaya más allá de la propia conservación y de las medidas de seguridad derivadas de esta obligación de conservación.

En este punto, querría recordar que el concepto de tratamiento en el contexto de la protección de datos tiene una configuración amplia, dado que se considera tratamiento cualquier operación o procedimiento técnico que permita recoger, grabar, conservar, elaborar, modificar, consultar, utilizar, bloquear o cancelar los datos, así como las cesiones de datos que se deriven de comunicaciones, consultas, interconexiones y transferencias de datos (art. 3, letra c de la LOPD, y art. 5.1, letra t del RLOPD).

Una vez abordada la cuestión del encargado del tratamiento, ya sea porque nos presta servicios de *cloud* de aplicación (software), de plataforma o de infraestructura, la segunda cuestión de relevancia que se debe tratar está relacionada con el hecho de que se pueda llegar a producir un movimiento internacional de datos como consecuencia del uso de servicios en la «nube». Si se da este supuesto, es de aplicación lo que prevé el título V de la LOPD (art. 33 y 34) y el título VI del RLOPD (art. 65 a 70).

Como principio general, se establece que no se pueden hacer transferencias de datos personales a países que no proporcionen un nivel de protección equiparable al de la LOPD.

Esta transferencia internacional se puede realizar si, además de cumplir lo que prevé la LOPD, así lo autoriza el director de la AEPD. El procedimiento para solicitar esta autorización lo regula el RLOPD (art. 137 a 144).

No es necesaria autorización si el país en el que se establece el importador de los datos ofrece un nivel adecuado de protección; esta determinación de nivel adecuado la efectúa el director de la AEPD, mediante resolución y para un país en concreto. Tampoco es necesaria esta autorización si el nivel adecuado ha sido declarado por una decisión de la Comisión Europea; aquí también se incluye, por ejemplo, el acuerdo de puerto seguro con Estados Unidos.

Asimismo, existe toda una serie de supuestos concretos que son excepciones a la necesidad de autorización del director de la AEPD. Estas excepciones se regulan en el art. 34 de la LOPD (tratados y convenios internacionales, auxilio judicial, servicios relacionados con la salud, transferencias dinerarias, consentimiento inequívoco del afectado, necesario en relaciones contractuales, interés público, procedimiento judicial o petición desde registros públicos).

En el supuesto de que la autorización sea necesaria, hay que presentar un contrato escrito, entre importador y exportador, en el que consten las garantías de respeto necesarias para la protección de la vida privada. A estos efectos existe un conjunto de decisiones de la Comisión Europea relacionadas con los contenidos de estos tipos de contratos (art. 70.2).

Las transferencias internacionales se deben notificar para inscribirlas en el registro general de protección de datos al registrar el tratamiento que prevé la transferencia internacional. Las autorizaciones de transferencias internacionales también se inscriben, en este caso de oficio.

Para las transferencias internacionales, pueden resultar de interés los estudios realizados por algunas organizaciones sobre los diferentes niveles de exigencia en materia de protección de datos.

Así, tenemos el mapa global de la protección de datos que desde hace unos años publica Privacy International,[www8] y otro nuevo que, con una cierta orientación de marketing, ha elaborado recientemente Forrester Research,[www9] acompañado de la pregunta de si sabemos dónde están nuestros datos en la nube (*Do you know where your data is in the cloud*?).

Por último, existe un caso especial de autorización de transferencia internacional, previsto en el art. 70.4 del RLOPD, para el caso en el que se produzca en el seno de grupos multinacionales de empresas. En tal situación, es necesario que estos grupos adopten lo que se conoce como BCR (*binding corporate rules*) o normas corporativas vinculantes, en las que consten las garantías de respeto necesarias para la protección de la vida privada y el derecho fundamental a la protección de datos, así como los principios y el ejercicio de derechos previstos en la LOPD.

Estas normas o reglas deben ser vinculantes para las empresas del grupo y exigibles según el ordenamiento jurídico español, y las puede exigir tanto la AEPD como las personas afectadas.

El grupo del art. 29 también tiene publicados algunos documentos relacionados con las BCR. A efectos introductorios, resultan de interés el «Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules», el «Working Document Setting up a framework for the structure of Binding Corporate Rules» y el «Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules», todos ellos de junio del 2008.

Según datos de la AEPD, entre el año 2000 y julio del 2007 se autorizaron un total de 148 transferencias internacionales, y en el 2007 se notificaron al registro de protección de datos 8.483 movimientos internacionales de datos.

[www8] http://www.privacyinternational.org/ y el mapa en http://www.privacyinternational.org/survey/dpmap.jpg.
[www9] http://www.forrester.com/rb/research y el mapa en http://www.forrester.com/cloudprivacyheatmap.

Por último, querría añadir una cuestión esencial relacionada con la protección del derecho fundamental a la protección de datos de carácter personal, en aquellas situaciones en las que éste se pueda ver vulnerado en ambientes de *cloud computing*, en los que se pueden dar situaciones de multiterritorialidad y, por lo tanto, con dificultades para resolver de manera efectiva las posibles vulneraciones; sin duda, es un tema que deberán abordar las autoridades de control, especialmente las de la Unión Europea, en cuanto a coordinación entre autoridades, intra- y extraeuropeas.

En resumen, los aspectos más relevantes relacionados con el cumplimiento legal que hay que abordar o tener en cuenta cuando conectamos protección de datos y *cloud computing* están relacionados con:

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

Cita recomendada

MIRALLES, Ramón (2010). «*Cloud computing* y protección de datos». 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-miralles/n11-miralles-esp›

ISSN 1699-8154

Sobre el autor

Ramón Miralles
ramon.miralles@gencat.cat

Coordinador de Auditoría y Seguridad de la Información. Autoridad Catalana de Protección de Datos.

Autoridad Catalana de Protección de Datos
C/ Llacuna, 166, 8.ª planta
08018 Barcelona, España

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

El teletrabajo: ¿Más libertad o una nueva forma de esclavitud para los trabajadores?

Carmen Pérez Sánchez

Fecha de presentación: octubre de 2010
Fecha de aceptación: noviembre de 2010
Fecha de publicación: diciembre 2010

Resumen
A pesar de los avances tecnológicos que han permitido la aparición de nuevas formas de trabajo en red, el teletrabajo –entendido como el trabajo remoto que implica el uso intensivo de herramientas telemáticas– representa actualmente un modo de organización del trabajo muy minoritario. Las resistencias para implementarlo por parte de las organizaciones son numerosas, pero también la experiencia y la valoración de los propios teletrabajadores es ambivalente. Por medio del análisis de las metáforas sobre el teletrabajo que hemos recogido en 18 entrevistas realizadas a teletrabajadores y teletrabajadoras con responsabilidades familiares, examinamos cuáles son las principales ventajas e inconvenientes de esta práctica laboral. Nuestro análisis muestra que si bien la capacidad para poder organizar los tiempos y los espacios de los diferentes ámbitos de la vida cotidiana (del trabajo remunerado, del trabajo doméstico y familiar, del ocio, etc.) de la manera que mejor convenga es el factor positivo más destacado por nuestros informantes, la posibilidad de estar permanentemente disponible para el trabajo, la familia, la casa y, por lo tanto, de no desconectar nunca se puede convertir también en su mayor riesgo.

Palabras clave
sociedad de la información y el conocimiento, TIC, teletrabajo, análisis del discurso, metáforas

Tema
Sociología del trabajo y las organizaciones

Teleworking: More freedom or a new form of slavery for workers?

Abstract
Despite the technological advances which have resulted in the appearance of new forms of online working, teleworking – working at a distance, using communication technologies – is still a very minor form of work organisation. There is a lot of resistance by organisations to put it into practice, but the experience and evaluation by teleworkers themselves is also ambivalent. By analysing the metaphors of teleworking from 18

interviews with teleworkers who have family responsibilities, we examine the main advantages and disadvantages of this work practice. Our analysis demonstrates that the most positive factor is the ability to organise time and space of daily life (for the job, household work, family, leisure, etc.) to best suit the teleworker. However, the possibility of being permanently available for work, the family and household tasks, which means never being able to disconnect, may also be the major risk.

Keywords
information and knowledge society, ICT, teleworking, discourse analysis, metaphors

Topic
Sociology of work and organisations

Introducción

Uno de los ámbitos en los que la irrupción de las tecnologías de la información y la comunicación (TIC) ha sido más estudiada es el laboral. Las TIC han favorecido la aparición de nuevas formas de organización del trabajo y seguramente la más importante es el trabajo en red. En el fondo, y tal y como nos recuerda Manuel Castells (1997), Internet es la forma de organización más habitual de la actividad humana a pequeña escala. Todo el mundo forma parte de alguna red: nuestro trabajo, nuestra familia, nuestros amigos, etc.; todas son, en potencia y en la práctica, nuestras mejores redes de apoyo. El surgimiento de Internet ha permitido la aparición de nuevas formas de trabajo y de coordinación a gran escala y ha sustituido las cadenas de mando lineales y centralizadas por un trabajo autoprogramable caracterizado por la ocupación formada, flexible y con capacidades de autoorganización (Vilaseca, 2004). De esta manera, el trabajo en red implicaría el paso de un contexto caracterizado por la estabilidad laboral y salarial a un sistema productivo y de trabajo basado en la flexibilidad. Esta flexibilidad, los modelos de trabajo variable, la diversidad en las condiciones de trabajo y la individualización de las relaciones laborales son las características principales del mercado de trabajo en la sociedad de la información y del conocimiento (Castells, 2001).

1. Origen y evolución del teletrabajo

Es dentro de este contexto –de implementación masiva de las TIC en el ámbito laboral donde debemos situar el teletrabajo. Aunque la mayoría de los autores sitúan el origen del concepto en el contexto de la crisis del petróleo de los años setenta, cuando Jack Nilles afirmó que «si uno de cada siete trabajadores urbanos no tuviera que desplazarse a su sitio de trabajo, Estados Unidos no tendría la necesidad de importar petróleo» (Nilles, 1976: 4), Peter Goldmark en su programa «La nueva sociedad rural» (1972; citado por Ortiz Chaparro, 1999) ya perfilaba este modo de trabajo.

Siguiendo a Eduardo Barrera, presidente de European Community Telematics/Telework Forum (ECTF), éste sería el inicio de una primera fase en la historia del teletrabajo que se extendió hasta mediados de los años ochenta, en la que los discursos de sólo unos miles de expertos, principalmente de Estados Unidos, se centraban en temas energéticos y medioambientales, es decir, el teletrabajo era una alternativa a la utilización generalizada del coche para ir al trabajo.

La segunda fase del teletrabajo se caracterizaría por la irrupción del PC y el desarrollo de las redes virtuales privadas, que fueron extendiendo el concepto de red local y generalizando el uso del correo electrónico. Respecto a las organizaciones, a finales de este período, que llegaría hasta comienzos de los años noventa, el teletrabajo aparece como una opción para dar apoyo al *outsourcing*, mientras que el desarrollo de la telefonía móvil digital y la bajada del precio de los ordenadores portátiles posibilitan la aparición de las primeras oficinas móviles.

Actualmente estaríamos en una tercera fase del teletrabajo, caracterizada por la globalización de la economía y la explosión de Internet, y más concretamente de la World

Wide Web. Esta globalización ha incrementado considerablemente la presión competitiva y la inestabilidad de los mercados, y ha obligado a las empresas a reconsiderar sus procesos productivos y a reclamar una mayor flexibilidad en el mercado laboral, mientras que por el lado de las infraestructuras hemos vivido un proceso de desregulación y privatización de las telecomunicaciones para potenciar la oferta y reducir costes.

El autor menciona una cuarta generación del teletrabajo que implicaría pasar a ser la manera habitual en la que la mayoría de las persona realizan, al menos parcialmente, su trabajo todos los días. Este cambio, que Barrera pronosticaba con la llegada del nuevo milenio, en el fondo significaría que el teletrabajo pasaría de ser considerado una manera innovadora de trabajar a ser la manera ordinaria de hacerlo.

La falta de estudios cuantitativos recientes no nos permite hablar de la evolución del teletrabajo en los últimos diez años, pero la Comisión Europea pronosticaba el inicio de una tendencia al alza de este fenómeno que «está llevando al cambio más sustancial en la práctica laboral desde hace mucho tiempo, que llegará a afectar a casi toda la población europea en alguna etapa de su vida laboral en los próximos cinco años y en los siguientes» (Status Report on European Telework, 1999: 126). Sin embargo, ni las predicciones para Estados Unidos –que hablaban de que la oficina se convertiría en un lugar para visitar de vez en cuando para recoger documentos y correspondencia (Blanco, 2006; Goldman, 2000)– ni para Europa se han cumplido. Así, W. J. Steinle afirmaba ya en 1988 que «hay más gente estudiando el teletrabajo que teletrabajadores reales» (1988: 8).

2. ¿Qué es el teletrabajo?

Esta evolución de la implementación del teletrabajo ha ido acompañada de diferentes conceptualizaciones. Así, revisando la bibliografía académica sobre el teletrabajo, nos encontramos con definiciones de carácter general para las que el teletrabajo sería un modo de trabajo remoto que implica el uso de las TIC (por ejemplo, Gillespie y Feng, 1996; Kerrin y Hone, 2001; Wikström et al., 1997). Sin embargo, lo que predomina son definiciones que se centran en aspectos más concretos del teletrabajo, como su posibilidad de reducir los desplazamientos de casa a la oficina, el papel de las tecnologías en la práctica del teletrabajo, el lugar en el que se debe realizar el trabajo remunerado o el régimen contractual que debe tener el teletrabajador[1].

En nuestro caso, hemos optado por trabajar con una definición amplia de teletrabajo según la cual éste sería el trabajo remunerado que cumpliera los siguientes tres requisitos:

- la ubicación: el trabajo se realiza en un lugar físico diferente de donde se necesitan los resultados,
- debe desarrollarse un uso intensivo de las TIC y
- debe existir un vínculo de comunicación con el empleador o contratista.

La falta de consenso en la definición del teletrabajo no deja de ser un síntoma más de que todavía estamos hablando de una modalidad de organización del trabajo muy minoritaria[2]. No obstante, la mayoría de los estudios, desde los más tempranos hasta los más recientes, señalan un conjunto de ventajas y de efectos beneficiosos del teletrabajo sobre las personas, las organizaciones y la sociedad en su conjunto. Así, por ejemplo, para las teorías postindustriales el teletrabajo liberaría a las personas de la disciplina y la alienación de la producción industrial. En este sentido, el trabajo remunerado en el hogar ofrecería la libertad del trabajo autorregulado y una reintegración del trabajo y la vida personal.

Por el contrario, también se han analizado ampliamente las resistencias por parte de las organizaciones a la hora de implementar esta modalidad de organización del trabajo, centradas principalmente en los costes, los cambios organizacionales y la inseguridad en la información. Desde esta perspectiva, autores como Richard Sennet han declarado que «el teletrabajo es la última isla del

1. Para una revisión más detallada de las diferentes definiciones del teletrabajo, ver PÉREZ, C. y GÁLVEZ, A. (2009). *Teletrabajo y vida cotidiana: Ventajas y dificultades para la conciliación de la vida laboral, familiar y personal*. Athenea digital, 2009 (15), pág. 57-79.
2. Según los estudios, se habla de que entre un 3 y un 8% de la fuerza de trabajo del Estado español realiza algún tipo de teletrabajo.

nuevo régimen», en el sentido de que el horario flexible, si se «ha de considerar una recompensa, también coloca al trabajador bajo el estricto control de la institución» (2000: 61). De hecho, el teletrabajo obliga a pasar de centrarse en la inversión (tiempo dedicado, manera de trabajar) a centrarse en el resultado (los resultados del trabajo) que, aunque no es una idea nueva, todavía genera muchas resistencias por parte de los directivos (Bailyn, 2006).

3. Metodología: El estudio del teletrabajo a través de las metáforas

Para analizar cuál es el impacto del teletrabajo sobre la vida cotidiana de las personas, hemos analizado 18 entrevistas en profundidad a teletrabajadores (9 hombres y 9 mujeres) con responsabilidades familiares. Para realizar el análisis del discurso nos hemos centrado en las metáforas que utilizan para referirse a la práctica del teletrabajo.

El lingüista George Lakoff argumenta en su libro *Metáforas de la vida cotidiana* que «el lenguaje se estructura metafóricamente» (1986: 42) y que estas metáforas tienen la capacidad de construir realidad, en el sentido de que nuestra manera de pensar, cómo actuamos, todo lo que experimentamos y qué hacemos en nuestra vida cotidiana es fundamentalmente de naturaleza metafórica. Por lo tanto, la metáfora constituye una manera de pensar el mundo y de organizar coherentemente un concepto mediante un vínculo analógico con un objeto o una imagen de otro orden, por lo que no es sólo un recurso retórico propio de un registro literario.

Asimismo, las metáforas sirven en gran medida para nombrar experiencias cotidianas con un lenguaje que nos es familiar, que simplifica, aunque normalmente hacen referencia a conceptos generales, abstractos y, en consecuencia, muchas veces ambiguos. En resumen, el recurso de las metáforas es un ejercicio de simplificación y generalización que trata de buscar imágenes que puedan describir la experiencia vivida. Aun así, no hemos de entender las metáforas como «una aproximación imperfecta» a una realidad que se quiere describir, sino como un recurso lingüístico que nos permite «entender el mundo que nos rodea y expresarlo» (Tusón, 2008: 7). En este sentido, también «la ciencia habla mediante las metáforas precisamente para descubrir y describir toda la complejidad de la realidad que estudia» (Cardús, 2009: 5).

Además, el hecho de que el teletrabajo no sea una práctica generalizada en las empresas y organismos públicos para la organización del tiempo y el espacio de trabajo provoca que todavía no encontremos metáforas consensuadas, repetidas y acordadas por todos nuestros informantes. Como veremos a continuación, a veces nos encontramos con metáforas que quieren describir una realidad y la contraria. Este hecho sólo hace que nos adentremos más en el juego de luces y sombras que supone la práctica del teletrabajo en la vida cotidiana de estos trabajadores. Podríamos decir, utilizando la metáfora de Bruno Latour (2001), que la práctica del teletrabajo no está «estabilizada»; todavía hoy en día no existe un consenso, un discurso homogéneo que describa lo que supone la práctica del teletrabajo –aunque los medios de comunicación en los últimos años están ayudando a construir una imagen muy determinada del teletrabajo.

Teniendo en cuenta estas premisas, a continuación analizaremos las metáforas que más se repiten a lo largo del discurso de las personas entrevistadas sobre el teletrabajo y que nos ayudan a conocer y comprender la valoración que hacen del teletrabajo y cómo viven en su vida cotidiana esta experiencia.

4. El teletrabajo como fuente de libertad

Para la gran mayoría de las personas consultadas, el teletrabajo supone la posibilidad de poder, en primera instancia, autoorganizarse el tiempo y el espacio de trabajo de la manera que más les convenga. De hecho, no dudamos en afirmar que esta libertad de poder decidir sobre la organización del tiempo propio, de decidir dónde y cuándo se trabaja, de poder establecer qué es importante y qué lo es menos, qué requiere más dedicación y qué se puede hacer en tiempos residuales, es la ventaja más valorada y más repetida por las personas que hemos entrevistado. En esta línea, la libertad que otorga el teletrabajo a los trabajadores, esta capacidad de autogestión, permite, como dice el siguiente entrevistado, que pueda trabajar a su aire, a su ritmo.

> **Trabajar a mi aire, a mi ritmo,** sin tener nadie aquí pegándome la colleja [...] Que eliges el horario que quieres, que trabajas las horas que... bueno, que mientras que tengas el trabajo hecho, pues lo haces en las horas que... que quieras. (Traductora).

Esta posibilidad de trabajar con el ritmo y en el horario que uno quiera repercute en gran medida en el resultado del trabajo realizado. Así, la gran mayoría de las personas consultadas afirman que cuando teletrabajan sienten que aprovechan más el tiempo, que son más productivos y que la calidad del trabajo realizado en casa es mucho mayor. Este hecho se debe principalmente a que en casa trabajan más tranquilos porque están solos y no tienen las interrupciones propias de la oficina: llamadas de teléfono, interrupciones de los compañeros, las pausas para el café, el tiempo de comer que se alarga, etc.

> Lo que siento es que **aprovecho muchísimo más el tiempo** que cuando vengo aquí. [...] Además de la tranquilidad, de la **tranquilidad** que tienes en casa, sin nadie, en mi caso, durante la mañana, aquí no. Es que estás con gente, teléfono, tal, diferente. (Profesor de universidad).

Teniendo presente que todas las personas entrevistadas tienen familiares dependientes a cargo, una cuestión que valoran muy positivamente del teletrabajo es que les ha permitido participar en actividades familiares que con un trabajo presencial no podrían. De hecho, con el teletrabajo el tiempo familiar no es un tiempo residual del tiempo de trabajo, no es aquel tiempo que queda «libre» después de la jornada laboral, sino que toma una centralidad muy valiosa para los padres y madres. De esta manera, los teletrabajadores afirman que por primera vez y gracias al teletrabajo han podido participar en actividades como llevar y recoger a sus hijos del colegio o de las actividades extraescolares, o poder ir a las reuniones escolares y tutorías. Los padres y madres, de esta manera, se sienten mucho más implicados en la vida de sus hijos: conocen mejor el colegio, sus profesores, los compañeros de clase y los padres y las madres de estos compañeros. También es muy importante la libertad que tienen para gestionar imprevistos relacionados con sus responsabilidades familiares, como cuando un hijo u otro familiar está enfermo, ya que pueden quedarse en casa para atenderlo o llevarlo con tranquilidad al médico. Los teletrabajadores son conscientes de que en aquel o aquellos días en los que el hijo esté en casa, o que necesiten acompañar a un familiar a realizar una gestión, seguramente no podrán dedicar tanto tiempo al trabajo remunerado, pero con la flexibilidad que les proporciona el teletrabajo saben que este tiempo lo recuperarán cuando la situación de emergencia o de excepción esté superada.

> Pero yo vivo fuera de Madrid, como a unos 20 kilómetros, más o menos, entonces, mmm... y luego tengo niñas pequeñas, que es el tema. A mí realmente lo que me interesaba era quedarme en casa algún día. Porque **yo lo que quería era llevarlas al colegio**, cosa que no he podido hacer nunca en mi vida (carcajada). Entonces, claro, algo tan tonto como esto, ¿no? (Jefa de área de la Administración del Estado).

Todos los padres y todas las madres valoran muchísimo esta mayor implicación en la vida de sus hijos y el resto de la familia gracias a la libertad de horarios que posibilita el teletrabajo. De hecho, es recurrente el comentario de que, anteriormente, cuando tenían un trabajo presencial debían pedir permiso al superior o pedir unos días de fiesta o de vacaciones para poder atender los compromisos familiares con la sensación de estar pidiendo favores o destinar los días de descanso a atender a los familiares para realizar un trabajo básico y necesario en nuestra sociedad: el trabajo de cuidado[3]. El estrés y la carga de culpabilidad que experimentan muchos trabajadores cuando tienen que faltar al trabajo por motivos familiares es enorme, sienten que no son buenos trabajadores, que no están dando el cien por cien a la empresa y se sienten en desventaja respecto a los compañeros que no tienen responsabilidades familiares o que, si las tienen, no se hacen cargo de ellas, un sentimiento que tienen muchas madres trabajadoras en relación con los hombres, tengan éstos hijos o no.

En este sentido, y relacionado íntimamente con este punto, los teletrabajadores enfatizan la tranquilidad que les da tener la opción de poder gestionar su tiempo libremente, ya que ello les ahorra el mal trago, si se nos permiten la expresión, de tener que dar explicaciones en el trabajo porque un día no se pueda asistir a éste por la necesidad de atender o realizar alguna gestión relacionada con el trabajo familiar.

3. Lo que desde la literatura del último tercio del siglo XX se venía llamando trabajo doméstico y trabajo familiar, en los últimos años, sobre todo desde los estudios feministas, se ha pasado a llamar trabajo de cuidado, para enfatizar la realización de algunas actividades necesarias para el mantenimiento de la familia fuera del hogar.

> O sea, que yo me pueda ir tranquilo a trabajar a la UB, **sin tener que dar cuentas a nadie**, a la biblioteca, o quedarme en casa para leer, donde aprovecho mucho más el tiempo, o si tengo que ir una mañana a ver la fiesta de mi hijo de la castañada o de los disfraces, porque sé que por la tarde o por la noche mi trabajo lo puedo hacer desde cualquier sitio, en este caso desde la universidad. ¿O qué mejor? Por lo tanto, me acogí al teletrabajo para esto, para acogerme a esa flexibilidad en la que yo creo. (Profesor de universidad).

Pero el teletrabajo no sólo permite poder organizar con más libertad el tiempo de trabajo remunerado, sino también el espacio en el que éste se realiza, tal y como muestra claramente la cita anterior, en la que el entrevistado explica que trabaja mejor en casa o en una biblioteca que en el despacho. La posibilidad que ofrecen las TIC de poder estar conectado desde prácticamente cualquier sitio y de contar con programas informáticos que permiten poder acceder desde cualquier terminal al contenido del ordenador de la oficina facilita que se pueda trabajar allá donde se esté y que, por lo tanto, también se pueda aprovechar mejor lo que con un trabajo presencial y sin estas tecnologías serían tiempos muertos. De hecho, la siguiente cita muestra claramente cómo la trabajadora ajusta su tiempo de trabajo para poder disponer de más tiempo familiar, concretamente con sus hijos, pero también cuando por motivos laborales debe viajar. De esta manera, el aeropuerto, el hotel, etc., pasan a ser también lugares de trabajo.

> Porque cuando estoy en Barcelona me gusta llevar a los niños al cole, porque viajo mucho, pues hay días que estoy... no sé, pues los lunes y los viernes pues llevar a los niños al cole, porque a mí me gusta involucrarme, ¿no? [...] Pero absolutamente paro, a mí me verás, absolutamente, puede a que a veces incluso ridículo, pero para mí es fundamental. Yo es que, como viajo mucho, **el aeropuerto para mí es la oficina**, por tanto, para mí, si voy en un viaje de negocios, aprovecho el tiempo de espera en el aeropuerto, o por la noche en el hotel me verás... Los viajes, siempre sé perfectamente lo que me cuesta el viaje en tiempo, por tanto, pues aprovecho para limpiar correo, preparar una reunión... [...] Un día me verás trabajando a unas horas un poco extrañas... Estoy en Barcelona, así que, por ejemplo, hoy mismo, a las cuatro y media, cinco menos cuarto, iré a buscar a los niños, estaré con ellos y ahora lo que haré es conectarme a las siete, o a lo mejor más tarde, a las ocho o a las nueve, depende de cuando los ponga a dormir, entonces me conecto. (Directora de una unidad de negocio de una empresa multinacional).

Por lo tanto, la metáfora del teletrabajo como fuente de libertad se concreta con otras metáforas que hacen referencia a la tranquilidad que da poder trabajar «a su aire», en el lugar que encuentren y en el momento más productivo, lo que permite tener la sensación de aprovechar mejor el tiempo de trabajo remunerado y, así, disponer de más tiempo para la familia. La clave está, en este caso, en la libertad de poder elegir, de poder decidir cómo organizar las 24 horas del día y cómo optimizar, de esta manera, el tiempo de trabajo remunerado y el familiar.

5. El teletrabajo como trampa

La capacidad de autoorganización de los diferentes tiempos de la vida cotidiana que proporciona la sensación de libertad antes mencionada también tiene su reverso, ya que, como todos sabemos, la libertad también implica una responsabilidad: la de saber utilizarla correctamente, saber administrarla. En este sentido, el teletrabajo se puede convertir en una trampa, ya que para la gran parte de los teletrabajadores consultados, el hecho de no tener un horario laboral rígido y unos espacios bien compartimentados dedicados a tareas específicas –la oficina para el trabajo remunerado, el hogar para la familia, el espacio público para el ocio, etc.–, sumado al hecho de la facilidad que proporcionan las TIC para poder estar conectado con el trabajo siempre y en cualquier sitio, supone el riesgo de tener que estar disponible las 24 horas del día y los 7 días de la semana para la organización para la que se trabaja.

Sin embargo, en muchos casos hemos observado que esta disponibilidad total no es tanto un requerimiento de la organización como una autoexigencia que se impone el trabajador, principalmente a causa de, en primer lugar, la falta de un horario de trabajo establecido que marque claramente un inicio y un final de la jornada laboral y, en segundo lugar, por la facilidad de poder estar conectado con los compañeros de trabajo a través de Internet o porque en todos los hogares de las personas consultadas hay al menos un ordenador que permite realizar el trabajo desde cualquier sitio y a cualquier hora. Por lo tanto, es habitual encontrar expresiones como «estar todo el día enganchado», «no desconectar nunca» o «irse la olla» para manifestar la sensación de tener que estar siempre pendiente de los requerimientos del trabajo, de estar continuamente consultando el correo electrónico o la mensajería instantánea.

> Pero yo veo a gente que sí que lo dice, que se le puede **ir la olla** con este tema, es decir, que **estás todo el día enganchado**. (Profesor de universidad).

Por lo tanto, ésta sería la «trampa» del teletrabajo. Se dispone de total libertad para gestionar el tiempo y el espacio de trabajo, pero el resultado es una sobrecarga de trabajo no sólo remunerado, sino también doméstico y familiar. El siguiente fragmento de entrevista muestra claramente este hecho. Para aquellos teletrabajadores que sólo trabajan desde casa uno o dos días a la semana, estos días se reservan para hacer todo el trabajo familiar y doméstico que hay pendiente, para poder recoger a los

hijos en el colegio, para pasar más tiempo con ellos, etc. Pero, al mismo tiempo, el trabajo debe hacerse igualmente y ello obliga perder tiempo de ocio o de descanso y tener la sensación antes mencionada de que no se desconecta en ningún momento.

> Nosotros no trabajamos por horas, trabajamos por objetivos, entonces tenemos que tener un trabajo hecho para un día y cómo lo hagas es tu problema. En ese «es tu problema», si tienes que hacer teletrabajo, pues... tú verás cómo lo haces, ¿no? Entonces, **el teletrabajo a veces es una ayuda y otras veces es una trampa**. Lo que a mí me pasa es... en ocasiones me quedo un día a la semana en casa, porque tengo muchas cargas familiares, y cuando no es que tengo que llevar a un niño al pediatra, tengo que llevar a hacer dos tutorías o, si no, generalmente, junto varias cosas en un día, entonces me quedo a trabajar en casa, lo que me pasa es que estoy todo el día arriba y abajo, y... que... bueno, que... trabajo poco, digamos, ese día... y... mi jefe, pues lo sabe, pero no le importa, ¿vale? Y ésta es la parte negociable del teletrabajo, ¿no? Que... no es que me coja un día de fiesta, realmente trabajo, pero trabajo muchísimo menos que si estuviera en la empresa. Y esto el *management* lo sabe, que normalmente si te quedas en casa, trabajas menos, la productividad es menor. [...] Entonces, aquí es donde viene el teletrabajo, que ya no es una opción, y que ya no es que tu jefe te lo dé, sino que te ves obligado a trabajar muchas noches. Y lo que... y lo que pasa últimamente, es... te facilitan tener ADSL, y te facilitan tener un equipo móvil, y si tú compras una impresora para tu casa, te la dan, y si... o sea, te facilitan tener todo el equipo para trabajar en casa, eso no es ningún problema, pero lo que te encuentras es trabajando más horas. (Ingeniera de una empresa multinacional).

Por lo tanto, como hemos visto en esta cita, en algunos casos la opción de teletrabajar sólo se adopta cuando el trabajador tiene compromisos familiares que atender y, por consiguiente, el día de teletrabajo se convierte en un día para realizar gestiones familiares o realizar trabajo doméstico, lo que provoca un gran estrés porque estas horas de trabajo se deben recuperar en otro momento, normalmente por las noches, cuando los hijos ya están durmiendo, o los fines de semana, cuando la pareja o los abuelos principalmente pueden hacerse cargo de ellos. El resultado es que no se desconecta en ningún momento y que la carga de trabajo total es mucho mayor que con un trabajo presencial en el que los límites de los tiempos y espacios, las tareas y las responsabilidades están mucho más definidas. Esta sensación de estrés, de no desconectar, de estar todo el día trabajando, provoca que, como en el caso de uno de nuestros informantes, se hable de situación «esquizofrénica».

> Es bastante **esquizofrénico**, porque el hecho de estar siempre allí... pues eso, que tienes la lavadora, que no sé qué, que el niño está enfermo, y el hecho de que tú estás allí, pues **no desconectas nunca**... de lo que es la cuestión doméstica. (Traductora).

Conciliar los diferentes ámbitos de la vida de una persona con las responsabilidades familiares –el trabajo, la casa, la familia, los amigos, etc.– requiere una organización de la vida cotidiana muy compleja que puede acabar convirtiéndose en un puzle en el que a veces cuestan encajar las diferentes piezas.

> No, lo que pasa es, eso, si te paras un momentito para hacerte un café, mientras te lo preparas, aprovechas para poner la lavadora. Que no sé, pierdes cinco minutillos, que muchas veces ya lo dicen, que de vez en cuando, trabajando, tienes que tomarte un descanso. Pues, ese descanso aprovecho y pongo lavadoras, hago no sé qué, que también repercute positivamente porque quiere decir que cuando terminas de trabajar, todo esto ya lo tienes hecho. Claro, esto llega a un punto... El otro día hacíamos como broma con el término *multitasquing*. Eso, las teletrabajadoras somos las reinas del *multitasquing*, porque estamos en todo, todo el rato. Entonces te vas organizando, chas, chas, a trocitos. **Es como si hicieras un puzle**. Ahora pongo esto, ahora hago esto otro, ahora aprovecho y... «aprovecho y» es como la frase de las teletrabajadoras. Aprovecho y... hago esto, y aprovecho y ahora haré esto. Y así vas organizándote, digamos. (Traductora).

En este caso, la entrevistada hace referencia a que son principalmente las mujeres quienes practican el «multitasquing», porque la mayoría siente que son ellas todavía las principales responsables del trabajo doméstico y familiar, teletrabajen o no. Pero esta sensación de que el tiempo se escapa cuando se trabaja en casa con la realización de las tareas del hogar también la hemos encontrado en algunos hombres, principalmente, aquellos que teletrabajan la totalidad de la jornada laboral. Así, en la siguiente cita, un padre habla de cómo el trabajo doméstico le absorbe de tal manera que las horas se le pasan muy rápido, sin poder haber hecho todo el trabajo que hubiera querido.

> **Se me pasa el día volando** y de trabajo trabajo no hago mucho. No sé si es lo que te estás encontrando pero **te absorbe la casa** muy fácilmente. [...] No es que no le dedique tiempo, lo que pasa es que se me va en cosas como hacer la compra, poner la lavadora... Bajas cinco minutos a hacer la compra y acaban siendo 45 minutos... Cualquier cosa, poner la lavadora, tender la ropa... A mí se me come mucho tiempo. Y no tengo casi nunca dos horas seguidas o tres horas seguidas para hacer una cosa. Muy pocas veces me pasa. (Gestor comercial y de proyectos).

Por lo tanto, ésta es la «trampa» del teletrabajo. La sobrecarga de trabajo remunerado, doméstico y familiar que padecen la mayoría de los teletrabajadores y la consiguiente ausencia de tiempo libre o de disposición personal, en muchas ocasiones, supone que se tenga la sensación de que no acaben desarrollando del todo como quisieran su papel de trabajadores, de padres, de hijos, de amigos, etc. Es decir, ni son buenos trabajadores, ni buenos padres, ni llevan la casa como les gustaría, ni tienen tiempo de calidad para estar con sus parejas, ni tiempo para dedicarlo al trabajo comunitario,

ni tiempo para ver a los amigos o realizar actividades de ocio.

> Esto implica un mayor estrés, no eres buena trabajadora porque al final **no estás haciendo ni una cosa ni otra**. (Socióloga y socia de una empresa).

En resumen, el efecto más perverso del teletrabajo, su trampa, es el riesgo de no desconectar nunca, de estar siempre disponible para el trabajo, todo el día «enganchado», y para la casa y la familia, que se «coman» el tiempo. Por lo tanto, el día a día se convierte en un no parar que se traduce en estrés y en un sentimiento de culpabilidad por no estar realizando ninguna de las tareas del todo bien.

6. Valoración global del teletrabajo

A pesar de estas imágenes negativas que las personas entrevistadas han asociado al teletrabajo, la gran mayoría se siente privilegiada por poder hacer parte o la totalidad de la jornada laboral desde casa, y organizarse el tiempo de la manera que más les convenga. Por lo tanto, esta sensación de privilegio puede ser interpretada de una manera general, en cuanto a la libertad que tienen para organizarse los tiempos de las diferentes esferas de la vida cotidiana o, en un sentido más restrictivo, bien porque son conscientes de que forman parte de una minoría de trabajadores que pueden acogerse a esta medida, bien porque el teletrabajo se ha conseguido gracias a una negociación entre dos partes, el jefe y el trabajador, lo que implica que se viva con el miedo a que, con un cambio de superior, de departamento o de categoría profesional, esta posibilidad les sea retirada. En el caso de organizaciones en las que la práctica del teletrabajo no es generalizada, la sensación de privilegio aumenta, ya que se comparan con los compañeros que deben trabajar presencialmente y valoran en mayor medida esta concesión.

> Soy consciente de que **soy una privilegiada**, ¿eh? Que... que... eso no se puede dar por descontado. [...] Yo firmo para que no me lo cambien. (Ingeniera de una empresa multinacional).

También hemos observado que la posibilidad de teletrabajar puede ser equiparada a una «promoción profesional». Tener la opción de trabajar parte o el total de la jornada laboral desde casa es, en muchas ocasiones, valorada mejor que un aumento de sueldo o una promoción dentro de la empresa. De hecho, muchos entrevistados han declarado no estar interesados en una promoción porque un cargo superior implicaría una dedicación mayor de tiempo al trabajo remunerado y, en la mayoría de los casos, a la renuncia al teletrabajo.

Así, en conclusión, la libertad que permite el teletrabajo para organizar la vida cotidiana, para poder atender mejor a los hijos u otros familiares dependientes, el hecho de no tener que dar explicaciones en el trabajo cuando se tienen compromisos familiares, a pesar del aislamiento y la pérdida de posibilidades de promoción profesional que ello puede provocar, si se nos permiten la metáfora, «no tiene precio».

> Yo creo que ya, en esta edad, y teniendo cargas familiares y tal, para mí, vamos, ha sido **la mejor promoción**. Yo... mira, bueno, yo he tenido mi subida y todo esto, pero aunque no me hubieran subido, **yo estoy bien pagada con esto, muy bien pagada**. (Analista programadora de una empresa multinacional).

7. Conclusiones

Mediante el análisis de las metáforas que las personas entrevistadas utilizan cuando se refieren al impacto o las consecuencias del teletrabajo en la organización de la vida cotidiana, podemos ver que sus experiencias como teletrabajadores no son ni totalmente positivas ni negativas, ni blanco ni negro, sino que se encuentran en un punto intermedio en el que el estrés por compaginar el trabajo doméstico, el familiar y el remunerado en una sucesión de tareas muchas veces simultáneas, el sentimiento de culpabilidad por sentirse unos privilegiados o por no poder llegar a todo, y el riesgo de restar opciones para la promoción profesional, no oscurecen del todo la gran ventaja del teletrabajo: la libertad de gestionar su vida de la manera que consideren más conveniente sin la necesidad de renunciar a ningún aspecto. Como hemos visto, en la mayoría de los casos, esta rearticulación de los tiempos se traduce en una disponibilidad mayor para lo doméstico y, sobre todo, para la familia. Las personas consultadas tienen claro que quieren estar en el mercado de trabajo, que el trabajo no es sólo una fuente de obtención de ingresos, sino también una manera de realizarse y sentirse mejor, pero por ello tampoco quieren renunciar a ser unos padres comprometidos con el trabajo de cuidado y de educación y el bienestar de sus familiares.

Bibliografía

BAILYN, L. (2006). *Breaking the Mold. Redesigning Work for Productive and Satisfying Lives*. Ithaca, Nueva York: IRL Press, Cornell Universtiy. 2.ª ed.

BLANCO ROMERO, A. (2006). *Teletreball, gènere i territori. Una comparació entre Catalunya, Ardèche i el Québec*. Barcelona: Generalitat de Catalunya, Consell de Treball, Econòmic i Social de Catalunya. 1.ª ed.

BARRERA, E. (1994). «Estado de situación del teletrabajo en Europa. Resultados de encuestas y estudios de casos». Teldet. Madrid: ECTF.

CARDÚS, S. (2009). «Tres metàfores per pensar un país amb futur» [artículo en línea]. Institut d'Estudis Catalans. [Fecha de consulta: 21 de junio del 2010]. <http://www.salvadorcardus.cat/files/091112DiscursIEC.pdf>

CASTELLS, M. (1997). *La sociedad red. La era de la información*, vol. 1. Madrid: Alianza.

CASTELLS, M. (2001). *La Galaxia Internet*. Barcelona: Plaza y Janés.

COMISIÓN EUROPEA (1999). *Estatus Report on European Telework* [informe en línea]. Bruselas. [Fecha de consulta: 21 de junio del 2010].

GILLESPIE, A.; FENG, L. (1994). «Teleworking, Work Organisation and the Workplace». En: Robin Mansell (ed.). *The Management of Information and Comunication Technologies: Emerging Patterns of Control*. Londres: Aslib. Pág. 261-272.

GOLDMAN, D. (2000). «Today's work and family issue: curbing abusive overtime». En: J. CASNER-LOTTO (ed.). *Holding a job, having a life: strategies for change*. Scarsdale, Nueva York: Work in America Institute. Pág. 175-179.

KERRIN, M.; HONE, K. S. (2001). «Job Seekers Perceptions of Teleworking: A cognitive mapping approach». *New Technology, Work and Employment*. Vol. 16, n.º 2, pág. 130-143.

LAKOFF, G.; JOHNSON, M. (1991). *Metáforas de la vida cotidiana*. Madrid: Cátedra.

LATOUR, Bruno (2001). *La esperanza de Pandora. Ensayos sobre la realidad de los estudios de la ciencia*. Barcelona: Gedisa.

NILLES, J. M. (1976). *The Telecommunications-Transportation Tradeoff. Options for Tomorrow*. Nueva York: John Wiley & Sons.

ORTIZ CHAPARRO, F. (1996). *El teletrabajo: Una nueva sociedad en la era de la tecnología*. Madrid: McGraw-Hill.

SENNET, R. (2000). *La corrosión del carácter*. Barcelona: Anagrama.

STEINLE, W. J. (1988). «Telework: Opening remarks on an open debate». En: *Telework: Present situation and future development of a new form of work organization*. Amsterdam: Elsevier. Pág. 7- 19.

TUSÓN, J. (2008). *Això és (i no és) allò*. Badalona: Ara llibres.

VILASECA I REQUENA, J. (coord.) (2004). *El teletreball a Catalunya: Conceptes, tipologies, mètriques i polítiques*. Barcelona: Generalitat de Catalunya, Consell de Treball, Econòmic i Social de Catalunya.

WIKSTRÖM, T.; PALM LINDEN, K.; MICHELSON, W. (1997). *Hub of Events or Splendid Isolation. The home as a context for teleworking*. Lund: Lunds University.

Cita recomendada

PÉREZ, Carmen (2010). «El teletrabajo: ¿Más libertad o una nueva forma de esclavitud para los trabajadores?». 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-perez/n11-perez>

ISSN 1699-8154

Sobre la autora

Carmen Pérez Sánchez
cperezsanchez@uoc.edu

Investigadora del IN3 de la UOC.

Universitat Oberta de Catalunya
Internet Interdisciplinary Institute (IN3)
Edificio MediaTIC
C/ Roc Boronat, 117
08018 Barcelona, España

IDP. Revista de Internet, Derecho y Política es una publicación electrónica semestral impulsada por los Estudios de Derecho y Ciencia Política de la UOC, que tiene como objetivo la comunicación y divulgación científica de trabajos de análisis e investigación sobre los retos y cuestiones que las tecnologías de la información y la comunicación plantean con respecto al derecho y la ciencia política.

IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA. N.º 11 (2010)

EDITA: Àrea de Comunicació. Publicacions a Internet. **DIRECCIÓN:** Eric Hauck. **DIRECTOR DE PUBLICACIONES EN INTERNET:** Lluís Rius **COORDINACIÓN EDITORIAL:** Maria Boixadera. **ASISTENTE DE EDICIÓN:** Margarita Perelló. **CORRECCIÓN Y TRADUCCIÓN DE TEXTOS:** Clara Ortega, Nita Sáenz (Eureca Media, SL), Shirley Burgess y Michael van Laake (inglés). **MAQUETACIÓN:** Maria Abad (Eureca Media, SL). **DISEÑO:** Elogia y Grafime. **ISSN:** 1699-8154. **DEPÓSITO LEGAL:** B-29.619-2005. **DIRECCIÓN POSTAL:** Universitat Oberta de Catalunya. Avda. Tibidabo, n.º 39-43. 08035 Barcelona. **DIRECCIÓN ELECTRÓNICA:** idp@uoc.edu. **WEB IDP:** http://idp.uoc.edu/

UOC
Universitat Oberta de Catalunya
www.uoc.edu