El "Cloud Computing" y la privacidad: un nuevo escenario

Eduardo Jacob
Profesor Titular de Ingeniería Telemática (UPV/EHU)

Hablar de "Cloud Computing" o computación en la nube, requiere en primer lugar consensuar a qué nos referimos. Hay muchas tecnologías y sus correspondientes aplicaciones para las que el calificativo parece adecuado y de hecho es empleado de manera generalizada: tenemos las fotos y la agenda en la "nube", tenemos un servidor de aplicaciones en la "nube"… Servicios como GoogleDocs, Picasa , Flickr o Dropbox forman parte de esa visión colectiva y en muchos casos inconsciente que tenemos de la "nube".

En este breve artículo queremos, sin embargo, referirnos a otro tipo de tecnologías. Probablemente una de las definiciones más acertadas y consensuadas de "Cloud Computing" sea la que proporciona el NIST (National Institute of Standards and Technologies) norteamericano en su documento "NIST definition of Cloud Computing V15" que viene a decir (de manera muy resumida) que: "El "Cloud Computing" es un modelo para proporcionar un acceso conveniente y bajo demanda a un conjunto configurable de recursos compartidos (por ejemplo: capacidad de almacenamiento, computación, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un esfuerzo mínimo de gestión o interacción con el proveedor del servicio". Esta definición, lógicamente, excluye de estas tecnologías servicios tradicionales de albergue de servidores.

Simplificadamente, desde el punto de vista de la infraestructura utilizada, esta "nube" puede ser privada cuando todos los recursos pertenecen a la organización que la utiliza, pública cuando todos los recursos pertenecen a un tercero e híbrida cuando por diversos motivos, se utiliza una arquitectura mixta en la que los recursos gestionados son tanto públicos como privados.

Existen diversos proveedores que están ya ofertando servicios comerciales. Tal vez los más famosos sean Amazon con sus servicios EC2 de computación elástica y S3 de almacenamiento escalable, Google con "Google App Engine" y Microsoft con "Windows Azure Platform". En general estos proveedores promueven su solución en base al ahorro respecto a una solución privada, a la garantía de que los datos están protegidos contra fallos catastróficos que podrían afectar a un único centro de proceso de datos, a la disponibilidad del servicio y a la mayor seguridad frente a ataques clásicos de seguridad. Probablemente todas estas reivindicaciones sean ciertas. Sin embargo es necesario recordar, que de acuerdo a estudios publicados recientemente, aplicaciones como el acceso a datos en movilidad o la integración de aplicaciones basadas en "Cloud Computing" constituyen un nuevo motivo para la adopción de estas tecnologías.

Sin embargo es necesario estudiar otras cuestiones que poco tienen que ver con la técnica. El "Cloud Computing" ha sido identificado desde la Comisión Europea, tanto por Viviane Reding, Vicepresidente Primera de la misma y Comisaria Europea de Justicia, Derechos Fundamentales y Ciudadanía en el documento "Keeping darkness out of the Cloud", como por Neelie Kroes, Vicepresidenta y responsable de la Agenda Digital, en su alocución titulada "Towards a European Cloud Computing Strategy", como una tecnología que conjuga unas potencialidades inmensas para el desarrollo de la Sociedad de la Información con unos retos no menores en el campo de la privacidad.

Hay infinidad de estudios realizados sobre la problemática que generan este tipo de servicios desde el punto de vista de la privacidad, entre estos podemos citar el de INTECO (Instituto Nacional de las Tecnologías de la Telecomunicación) "Riesgos y Amenazas en Cloud Computing", el de ENISA (European Network and Information Security Agency) "Security and Resilience in Governmental Clouds" orientado a las administraciones públicas y traducido recientemente por INTECO, el del NIST "Guidelines on Security and Privacy in Public Cloud Computing", y del WPF (World Privacy Forum) "Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing". Incluso se han creado instituciones como la CSA (Cloud Security Alliance) y su correspondiente capítulo español, dedicadas a esta problemática. A continuación, destacamos los aspectos de esta tecnología que más influencia e impacto tienen en las cuestiones relativas a la privacidad.

-El primero y más inmediato es que los datos pueden "moverse" por razones de servicio por los diversos servidores que constituyen la infraestructura del proveedor, pudiendo éstos residir

en distintos países. Por otro lado, debido al proceso mismo de replicación, no se puede garantizar la existencia de una única copia de los datos. Finalmente, no se contempla como parte del servicio comunicar la localización actual de los datos y sus copias. Los problemas que esto genera son los siguientes:

- La normativa que regula el acceso a los datos por parte de terceras partes puede variar con la localización de los mismos, por lo que esto introduce la variable temporal en el estudio de la normativa aplicable, por ejemplo, en el campo de la privacidad, de la confidencialidad, de las medidas de seguridad a tomar, del acceso por parte de representantes de la ley o de la sede legal del prestador del servicio.

- La posible existencia simultánea de los datos en más de un sitio puede complicar la determinación de responsabilidades en caso de cesión o fuga de datos y genera además conjuntos de normativas aplicables en paralelo.

- El segundo es que el almacenamiento y procesado de información de terceros en estos sistemas puede definir escenarios en el campo de la confidencialidad y privacidad de la misma que no suelen estar recogidos tradicionalmente en los contratos de prestación de servicio entre empresas.

- El almacenaje de datos de carácter personal de terceros (y de los propios trabajadores de la empresa) en un servicio de "Cloud Computing" puede ser considerado como una cesión no autorizada de datos de carácter personal.

- El almacenaje de datos de carácter confidencial en estos sistemas puede ser considerado como una violación del contrato o del deber de secreto.

-El tercer aspecto es compartido con cualquier aplicación que implica el uso de Internet y es relativo a la modificación y/o eliminación de los datos.

- No es posible garantizar el borrado o la actualización de todas las copias que puedan existir de datos. Se habla del "Derecho a ser olvidado" como una de las cuestiones pendientes de Internet. Esto es especialmente importante para la finalización de contratos o en el caso de cesiones autorizadas de datos personales como mecanismo para implementar el derecho a la rectificación y cancelación de los mismos.

Es por esto que es imprescindible profundizar en un marco que regule tanto el despliegue de los servicios de "Cloud Computing" como la contratación de los mismos, definiendo claramente el flujo permitido de información, la política de privacidad que tiene que ser aplicable y aplicada a todas las localizaciones y que promueva una transparencia en el tratamiento de los datos. Una vez más, la particular normativa estadounidense en el campo de la privacidad y el hecho de que los precursores de estas tecnologías estén radicados allí, dota de una complicación adicional al problema, a la vez que da pie a implementaciones europeas del servicio que sean más adecuadas al tratamiento de la privacidad que se da en la Unión Europea.