Por Ley

Externalización de servicios a través de Cloud Computing

Por Ricardo De Lorenzo

Jueves, 07 de marzo de 2013, a las 20:34

La adopción de los servicios de Cloud Computing, es una realidad latente en las empresas españolas, y en concreto en el ámbito sanitario donde los procesos de informatización son cada día más avanzados. Dichos servicios suponen un importante ahorro de costes, agilidad en el envío y recepción de datos y comodidad de acceso por parte del usuario. Ahora bien, a la hora de adoptar estos servicios de Cloud Computing surgen numerosas cuestiones, entre las que predominan las relativas a la materia de protección de datos de carácter personal, dado que los mismos suponen en la mayoría de las ocasiones la realización de transferencias internaciones de datos.

Las transferencias internacionales de datos se definen en el artículo 5.1.s.), del Real Decreto 1720/2007, de desarrollo de la Ley Orgánica de Protección de Datos, como un tratamiento de datos que supone una transmisión de los mismos fuera del espacio económico europeo, estableciéndose por tanto, como principio general la prohibición de las mismas fuera de la Unión Europea, salvo el caso de países que ofrezcan un nivel de protección equiparable, de acuerdo con los criterios de la Agencia Española de Protección de Datos.

Para el resto de países, deberán de aplicarse medidas de protección equiparables a las de la Unión Europea, a través de solicitud de autorización por parte del Director de la Agencia Española de Protección de Datos, a la que se añada un contrato escrito celebrado con el proveedor del servicio de Cloud Computing extranjero, que deberá contener las garantías necesarias en materia de protección de datos, de acuerdo con una cláusulas tipos aprobadas por la Comisión Europea contenidas en la Decisión 2010/87/UE, siendo también aplicables para proveedores norteamericanos adheridos a los principios de puerto seguro, de acuerdo con la Decisión 2000/520/CE.

Lo hasta aquí visto sobre las transferencias internacionales de datos nos lleva a concluir que el proveedor de Cloud Computing tendrá como obligación principal notificar la ubicación de los datos, con el fin de que la empresa pueda determinar si son llevados o no a un país con protección equiparable.

El mayor inconveniente que surge en la contratación de estos servicios es el desconocimiento por parte del propio proveedor, en la mayoría de las ocasiones de la efectiva ubicación de los datos, pues los mismos pueden estar repartidos en múltiples servidores subcontratados produciéndose un incumplimiento en materia de seguridad, dando lugar a que la empresa no pueda verificar si se hallan en un país que ofrece una protección equivalente a la Unión Europea.

Estos supuestos, han exigido una revisión en el ámbito legislativo de las medidas de seguridad que deben adoptarse en las transferencias internaciones de datos, con iniciativas tales como acuerdos intergubernamentales y nuevas regulaciones de la materia de protección de datos, para que en casos como el anteriormente expuesto no se produzca un incumplimiento de las garantías mínimas exigidas o la paralización de las transferencias internaciones de datos, produciendo un retroceso en la globalización de las redes de telecomunicaciones.

Por todo ello, y a la espera de la entrada en vigor de estas medidas de flexibilización que revisen los actuales requisitos de seguridad para las transferencias internacionales de datos, los servicios de Cloud Computing contratados, deberán ser inspeccionados previamente, a fin de verificar que los datos se encuentran en la Unión Europea, en países con niveles equiparables, o por el contrario en otros carentes de tal protección acarreando un incumplimiento normativo grave.