# *CLOUD COMPUTING. SUS DILEMAS LEGALES.*

Pablo García Mexía
Profesor de Derecho de Internet
(The College of William & Mary)
Letrado de las Cortes

## I. DERECHO Y NUBE

El mundo tecnológico y la industria que promueven la generalización de la computación en nube muestran un vivísimo interés por sus perspectivas legales.[1] Parece lógico, dada la novedad y gran calado de esta tecnología.

Ahora bien, el impacto jurídico de la computación en nube es muy diverso, en función del estrato de Internet al que concierna. En lo que hace a la red y soporte físicos, es natural que apenas se vean afectados, al quedar en todo caso al margen de cualquiera de las tres modalidades de servicio que la cloud puede implicar (infraestructura, plataforma o software). Donde ese impacto resulta en cambio capital es en los otros dos estratos de la Red: código y contenidos.

## II. CLOUD Y CÓDIGO

En punto a ese primer estrato, es verdad que la cloud computing respeta plenamente los estándares y protocolos instalados sobre TCP/IP. Aunque también que la paulatina y creciente configuración de nubes "cerradas" podría poner en peligro el principio de neutralidad de la Red: el hecho de que un cliente o usuario de servicios en nube no pudiera sencillamente "portar" sus datos sin trabas entre uno u otro proveedor cuestionaría de lleno aquel postulado, de ahí que comiencen ya a oírse voces en favor de

[1] *Cfr.* http://channel9.msdn.com/posts/channel9spain/Implicaciones-legales-del-Cloud-Computing/; http://egap.xunta.es/detalleRecurso.php?id=358.

la *cloud neutrality* y de la necesidad de configurar la portabilidad de los datos como un derecho legalmente previsto.

## III. CLOUD Y CONTENIDOS DE INTERNET

En cualquier caso, el estrato de Internet que en mayor medida acusará el impacto legal de la computación en nube es el de sus contenidos, es decir, los datos en forma de texto, voz, imagen, vídeo, etc., que la Red fue diseñada para transportar.

### *1. Cloud y libertades*

El de los *derechos y libertades* es probablemente el campo sobre el que la cloud computing se refleja con mayor contundencia, siendo dos sus principales dimensiones concretas.

Una es sin duda la de la *protección de datos*. Con las leyes españolas en la mano, el cliente de nube no pierde su condición de responsable de los ficheros, de los que por lo tanto habrá de dar cuentas a pesar de haberlos puesto a disposición del proveedor; éste, por su parte, será entonces un mero encargado (externo) del tratamiento, sujeto a las instrucciones (en particular de seguridad) que el cliente/responsable considere oportuno impartir. A la vista de lo dicho, es pues fundamental que todo cliente de servicios en nube elija con sumo cuidado al proveedor, tratando de asegurarse de que conoce y efectivamente aplica la muy exigente normativa sobre protección de datos vigente en la Unión Europea y en nuestro país.

Dos problemas adicionales al hilo de este derecho fundamental: el primero, las transferencias extra-comunitarias de datos, que podrían redundar en lesiones de derechos, derivadas del hecho de que los datos terminaran recalando en jurisdicciones menos protectoras. Volveremos sobre ello más adelante.

El segundo, los registros por poderes públicos del proveedor de servicios en nube. En este punto, nuestra legislación –como en general todas las occidentales- presenta una

clara laguna, al haber sido diseñada en tiempos en los que esta modalidad computacional sencillamente no existía. Así lo revela el hecho de que la protección en favor del titular de los datos que ha confiado en un proveedor de nube para su tratamiento sea inferior en este concreto aspecto de la que se le prestaría en el caso de que los datos permanecieran en el disco duro de su propio ordenador (personal o corporativo): ello se debe a que, de ser requerido para ello, el proveedor de nube debería entregar esos datos a las fuerzas de seguridad, aun cuando se reservara la posible impugnación ulterior de la legalidad de tal registro.

El segundo campo de relevancia en materia de derechos y libertades es el de la *responsabilidad por contenidos* que pudieran redundar en lesiones de derechos de terceros. La normativa en vigor, que se aplica a los prestadores de servicios de la sociedad de la información, diseña un triple escenario de responsabilidad –ascendente-, en función de que la labor de ese prestador consista en la mera transmisión de datos (lo que hace un proveedor de acceso a Internet, Telefónica, sin ir más lejos), en la realización de copias-caché exigidas por la propia transmisión (la misma Telefónica, a fin de mejorar el servicio de ADSL que presta a su clientes, por seguir con el ejemplo) o en el almacenamiento de datos (de nuevo esa empresa de telecomunicaciones, respecto de una página web de un cliente, alojada en sus servidores).

Ahora bien, la computación en nube implica por naturaleza una modalidad de servicios de la sociedad de la información que va incluso más allá del almacenamiento, siendo, eso sí, a esta última (y no a las dos anteriores), a la que más semejante resulta. Por consiguiente, el régimen de responsabilidad por contenidos que se deberá aplicar a los servicios en nube habrá de ser por analogía el propio del almacenamiento, si bien resulta a mi juicio necesario que el legislador europeo (y subsiguientemente el español) prevea un régimen específico de responsabilidad propio de la cloud computing, obviamente agravado para el proveedor respecto del existente para el almacenamiento.

*2. Cloud, ciberseguridad y cibercrimen*

Por su propia esencia (los datos no residen "bajo techo" del cliente, sino en los servidores del proveedor de nube…), la cloud computing entraña riesgos agravados de seguridad, y por ende, de *cibercriminalidad* (el reciente episodio Google-China, a raíz del "hackeo" de las cuentas -en nube- de Gmail es buena muestra de ello). La necesidad de extremar la diligencia en este ámbito, tanto por parte del cliente como del proveedor de servicios en nube, se revela pues evidente.

*3. Cloud y jurisdicción*

Finalmente, la *jurisdicción*, probable fuente de las cuestiones jurídicas de mayor complejidad planteadas por Internet, dada su ubicuidad, de alcance planetario. Una complejidad que la nube, al potenciar esa ubicuidad (de proveedores directos o indirectos; o de los datos), seguramente va a incrementar.

El Estado queda pequeño para afrontar tamaño desafío jurídico. Al tiempo, no sólo es inviable por idealista, sino incluso indeseable, prescindir de las culturas y valores nacionales de casi 200 Estados, a fin de lograr tratados internacionales orientados a proporcionar soluciones justas.

Bien es verdad, por otra parte, que cifrar al azar de la residencia, paradero (de personas o bienes) o potencial extradición la efectiva aplicación de una norma que la computación en nube pudiera exigir es una opción sin duda realista, pero también potencialmente injusta.

Un tercer posible orden de soluciones no parece en cambio injusto, pues sujeta a un criterio tan objetivo como razonable la vigencia de una concreta jurisdicción: el estrictamente derivado de la presencia de los servidores "de nube" en un específico Estado. Este argumento, que encuentra respaldo en la normativa española, resulta a la vez realista, pues un prestador europeo puede, por ejemplo, soslayar de ese modo el problema antes mencionado de la transferencia de datos a Estados que cuenten con estándares inferiores de protección; así lo hacen algunas de las empresas más relevantes del sector (Microsoft, por ejemplo).