

05/09/2022

Julio V. González García

La instauración de un *cloud* para el sector público resulta una necesidad para la modernización de las administraciones públicas. De hecho, son numerosos los contratos y las previsiones de contratos públicos para la provisión de este servicio que van a necesitar desde el Gobierno de la nación al más pequeño de los ayuntamientos, pasando por el sector público empresarial, el institucional o el fundacional. Una necesidad que está muy vinculada a la legislación de contratos del sector público, con lo cual es preciso abordar, de forma inicial, una serie de cuestiones.

Dos mitos y un dato sobre la contratación del cloud

Las cuestiones cibernéticas se suelen examinar como elementos virtuales, que están deslocalizados, con lo que no resulta necesario su ordenación jurídica en el mercado interior.

Primer mito.

Sin embargo: la realidad aparente es que nos encontramos ante problemas de gestión de bienes materiales: los **servidores** ya que lo que se acostumbra a ver son los instrumentos en los que se ubica. **Segundo mito que lleva a considerar un suministro.**

Pero, realmente, cuando estamos haciendo referencia al *cloud*, **la cuestión central es de servicios**, los que permiten la gestión de los datos. Una cuestión que hace que nos encontremos ante un **contrato mixto**, cuya parte primordial sean los servicios incorporados, que proporcionan valor añadido.

En efecto, en los contratos de cloud se acostumbran a incluir seis servicios básicos y dos servicios avanzados: servicios de computación (dentro de los cuales, se incluyen, además, números servicios incorporados como modalidades de la computación), almacenamiento, servicios de red, servicios de recuperación de datos perdidos en caso de daño, servicios de seguridad y servicios de comunicaciones para la empresa suelen estar incluidos en todos los contratos de cloud.

Por todo ello, tal como señalé [en otra ocasión](#), discrepo del parecer de la Junta Consultiva de la Contratación Administrativa, en su [Informe 13/2021, de 10 de junio](#).

Tres aspectos sobre el futuro del cloud en el sector público

El presente generará numerosas situaciones en las que el sector público licitará contratos de cloud. Pero será preciso un cloud que no sólo lleve al almacenamiento de datos sino que permita prestar servicios de computación para la gestión de estos datos que el sector público tiene que proveer de forma necesaria. Es lo que permitirá superar viejas concepciones de la

recaudación, de la intervención o incluso de los servicios jurídicos.

Ahora bien, no toda la contratación de servicios de *cloud* aplicará la LCSP sino que tendremos que introducir las reglas de la Ley 24/2011, de 1 de agosto, de contratos del sector público en los ámbitos de la defensa y de la seguridad. De hecho, parte de los contratos más atractivos que van a surgir en el futuro se tienen que desarrollar en el ámbito militar y de la seguridad. Un ámbito en el que se incrementan las necesidades de seguridad, por lo que el papel del CCN será especialmente significativo.

En un futuro próximo, el sector público podrá ser prestador de servicios de *cloud*, para particulares y para el sector público; que serán los aspectos que se desarrollan en las líneas siguientes.

Cinco retos esenciales para la adjudicación de contratos de cloud en el ámbito público

1. Los contratos de *cloud computing* supone la realización de un proyecto característico y propio para las entidades del sector público, no replicable. Por ello, resulta necesario plantearse si se pueden considerar los contratos de *cloud* contratos excluidos por razón de propiedad intelectual.
2. Desde este punto de vista, resulta necesario evitar que los datos lleguen a terceros países, evitando la fuerza expansiva de normas extranjeras como la CLOUD ACT de los EE.UU. que obliga a la entrega a las autoridades estadounidenses de los datos que soliciten que estén en servidores de empresas radicada en EE.UU., con independencia del lugar de ubicación de los servidores. El derecho estadounidense sigue a la empresa, con independencia de donde se ubiquen.

Lo anterior ha de configurarse como un criterio de participación en la licitación y debe afectar a todas las empresas de terceros países que tengan legislación como la descrita.

De hecho, el Gobierno francés acaba de prohibir la utilización de Microsoft Office 365. ¿Nos debemos plantear, en este sentido, que, por ejemplo, Google deje de proporcionar *gratuitamente* las plataformas de correo electrónico y sus suites complementarias a las Universidades públicas españolas? Debemos pensar, en este sentido, que toda la política general de usuarios de Google es similar al que se suministra al usuario universitario.

3. Desde el Sector público hay que potenciar la consecución de la soberanía digital y garantizar la participación en el reparto de la riqueza vía impuestos. Aquí se ha de garantizar la sostenibilidad del contrato entendida en el sentido de que las empresas adjudicatarias han de tributar en el lugar de producción de la riqueza.
4. Hay, en cuarto lugar, que establecer una regulación conveniente del lugar de instalación de los servidores a fin de garantizar un adecuado nivel de protección ambiental de los servidores. Es una vertiente de la sostenibilidad del contrato.
5. Cumplimiento de las exigencias de la Estrategia Nacional de Seguridad, reformada en 2021: el papel del Centro Criptográfico Nacional, en la medida en que hay que garantizar un alto nivel de seguridad, para la protección del interés general y de los derechos de los particulares.

El cloud, la defensa y la seguridad

La defensa y la seguridad se gestiona esencialmente a través de elementos electrónicos, dentro del cual el cloud es básico. Una seguridad que sirve, además, como instrumento para la realizaciones de actividades instrumentales para la defensa y la seguridad. Y que en el futuro necesitará

En este sentido, se trata de un contrato excluido de la Ley 24/2011, ya que el *cloud* se encuadra en su artículo 7.1. b) “Aquellos contratos que de regirse por la presente Ley, resultaría necesario revelar información contraria a los intereses esenciales de la Seguridad, o bien conforme al artículo 346 del Tratado de Funcionamiento de la Unión Europea, pudieran resultar perjudicados los intereses esenciales de la Defensa o la Seguridad Nacional”.

Conexión con la seguridad física: el papel del Centro Nacional de Protección de Infraestructuras Críticas para la protección del lugar en el que se ubiquen las infraestructuras necesarias para la protección del *cloud*.

Un servicio prestado por el Estado

Como ya he tenido ocasión de señalar en otra ocasión, la empresa pública es el mecanismo más eficaz para garantizar la autoprovisión de servicios de *cloud* a las Administraciones públicas ya que es lo que permite superar de la mejor manera los retos a los que se enfrenta el sector público en el mercado de *cloud*. Especialmente lo relativo a la soberanía de los datos en territorio español.

En efecto, la empresa pública es una forma eficaz y exigente de garantía de los datos críticos de seguridad nacional La empresa pública es una forma adecuada para proveer de estos servicios a los operadores económicos manteniendo la soberanía digital del país, garantizando la territorialidad de los datos y los secretos empresariales.

Frente a los problemas que plantean las empresas estadounidenses, ya que este país no es un puerto seguro en materia de datos personales, constituye una forma adecuada de incorporar un alto nivel de protección de datos de carácter personal.