¿Dónde están mis datos?

La custodia de datos de la administración española

Alberto Fraile Sastre

Nunca os habéis preguntado... ¿dónde se guardan mis datos?, ¿quién puede acceder a ellos? o ¿quién los gestiona? Pues bien, todas las respuestas tienen un foco común, la Administración General del Estado. Dicha Administración, en la actualidad, ha cambiado los archivos físicos por otros formatos más eficientes, baratos y seguros como la nube informática, donde reparte su espacio disponible entre los diferentes organismos a su cargo contándose en la actualidad con 24.580 servidores. De entre ellos, según el último informe REINA, el Ministerio de Empleo y Seguridad Social es el que más posee al contar con 5.881 servidores.

Pero con tantas instituciones y equipos de almacenamiento… ¿puede conocerse donde se encuentra la información de una persona en particular y quien gestiona dicho servidor? En principio la respuesta sería si, puesto que según la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), el derecho de acceso está reconocido pero, por desgracia, también existen determinadas restricciones como que el responsable del tratamiento de datos no está obligado a revelar la ubicación del centro de almacenamiento, la existencia de encargados, etc.

Si se pregunta a diversas instituciones donde guardan sus datos y quien se encarga de su gestión se pueden obtener respuestas como la del Ministerio de Empleo y Seguridad Social, donde afirman que su Gerencia Informática es la encargada de crear, custodiar y administrar sus bases de datos mientras que, realmente, en 2014 transfirieron los servicios de operación, gestión y soporte técnico de sus sistemas de información a la unión temporal de empresas formada por INSA, GESEIN, SOFTWARE AG y SIA.

Por otra parte, el Ministerio de Justicia cuenta con diferentes centros de procesamiento de datos, mientras que la Subdirección General de Nuevas Tecnologías de la Justicia posee dos centros de datos en Madrid que el departamento de justicia otorgo a la consultora SATEC para realizar sus servicios de mantenimiento, gestión y desarrollo.

En el caso de la Agencia Tributaria, esta presenta una infraestructura tecnológica que permite la gestión de los datos que recibe mientras que el Ministerio de Hacienda y Administraciones Públicas posee centros de datos en diferentes puntos de Madrid a los que se deben sumar dos centros adscritos al Departamento de Informática Tributaria. Eso sí, la Agencia Estatal de Administración Tributaria también utiliza la unión temporal de

empresas de INSA, GESEIN, SOFTWARE AG y SIA para que gestione y administre sus datos, sistemas y aplicaciones.

En cambio, los datos del DNI electrónico son tarea de la Policía Nacional, quienes utilizan un único centro de datos para España que es administrado por su Gerencia Informática.

Podemos observar, por tanto, que en la mayoría de instituciones de la Administración Pública se cuenta con uno o varios centros de datos propios pero que su gestión y mantenimiento ha pasado a manos de empresas privadas, lo cual puede conllevar problemas de seguridad o la pérdida del control sobre la información. Por ello, la Agencia Española de Protección de Datos (AGDP) asegura que las medidas de seguridad son imprescindibles para garantizar la integridad de los datos personales, evitar accesos no autorizados, recuperar la información, etc.

Además, la posibilidad de que existan estos problemas de seguridad provoca que, cuando los organismos recurren a empresas externas, sea fundamental revisar las condiciones para garantizar el mínimo riesgo tecnológico y jurídico. Por ello, las concesiones de la Administración deben ser de consulta pública y registrarse en ellas un acuerdo de nivel de servicio que garantice sus prestaciones. Además, deberá probarse su cumplimiento a través de auditorías y certificados como los de EUROCLOUD, Cloud Security, etc., así como a través de auditorías técnicas realizadas por el cuerpo de informáticos de la propia Administración.

Por último, desde la Administración aseguran cumplir con las medidas de protección exigidas en la legislación y creen en las ventajas de los servicios de Cloud Computing que cada vez generan mayores garantías frente a ataques o pérdidas así como beneficios en interoperabilidad, eficiencia y ahorro de espacio.■