Informe 0457/2008

La consulta plantea qué medidas debe adoptar el responsable que ha contratado la prestación de un servicio que comporta el tratamiento de datos personales por un tercero encargado para asegurarse que éste cumple con las garantías exigidas por la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal y su Reglamento, Real Decreto 1720/2007, de 21 de diciembre.

I

La consulta se refiere en concreto a lo dispuesto en el artículo 20.2 del Reglamento, Real Decreto 1720/2007 que dice: "Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este reglamento."

Por otra parte, en el Título VIII del Reglamento desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal, figurando entre estas medidas la elaboración e implantación de la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

La Ley Orgánica 15/1999 establece en su artículo 9. 1 que"el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural." En su número 2 dice que "No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas."

A su vez el artículo 12. 2 de dicha Ley señala que “La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar”. En su número 3 dice que “Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto de tratamiento.” Su número 4 señala por último, que “En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.” En el mismo sentido se pronuncia el artículo 20.3 del Real Decreto 1720/2007, añadiendo que” No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiere encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.”

A su vez, el artículo 12 de la Ley trae causa del artículo 17 de la Directiva 95/46 del Parlamento Europeo y del Consejo de 24 de octubre de 1995 referido a la seguridad del tratamiento, cuyo número 2 señala que “Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamientos por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas”. Y su número 3 dice que “La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento.

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.” Por último, su número 4 establece que “A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 (medidas técnicas y organizativas) constarán por escrito o en otra forma equivalente.”

La conclusión de la regulación citada es la de que el encargado debe limitarse a tratar los datos por cuenta del responsable y de acuerdo con sus instrucciones (….como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita su ámbito de actuación para la prestación de un servicio, según reza el artículo 5 del Reglamento). De modo que la exigencia de contrato escrito en el tratamiento de datos personales por cuenta de tercero con el contenido determinado por el articulo 12 de la Ley Orgánica constituye un requisito de garantía y de que el tratamiento de datos así estipulado no supone una comunicación inconsentida de datos por parte del cedente y un tratamiento indebido por parte del tercero cesionario, atendiendo a lo dispuesto en los artículos 6 y 11 de dicha Ley, que podría dar lugar a la aplicación del régimen sancionador contemplado por el artículo 43 de la Ley. La obligación que incumbe al responsable del tratamiento de datos de no ceder o comunicar datos a un tercero para que los trate por su cuenta se entenderá cumplida cuando, tras elegir a este encargado de tratar los datos, las relaciones entre ambos, en lo que respecta a la protección de datos personales, se instrumente el contrato escrito o cualquier otra forma que permita acreditar su celebración, en el que figurarán las medidas técnicas y organizativas que la otra parte del contrato, el encargado, estará obligado a cumplir desde el momento de su suscripción.

Cabe resaltar entre la numerosa jurisprudencia sobre el artículo 12 de la Ley 15/1999, la STS de 17 de abril de 2007 que ha resaltado la finalidad de este artículo y en particular de los rigurosos requisitos que se establecen en relación con el contrato en él regulado: " lo que necesariamente exige una forma que refleje y deje constancia no sólo de su celebración sino de su contenido, que incluso se especifica en sus cláusulas imprescindibles en el propio precepto. Tal exigencia responde a la finalidad de la norma de garantizar que el acceso de terceros a los datos de carácter personal, objeto de tratamiento automatizado, se produzca únicamente en los casos y con las limitaciones legalmente establecidas, plasmándose las condiciones, finalidad y alcance de la cesión de forma que resulte controlable en su desarrollo y cumplimiento."

II

En el Reglamento, Real Decreto 1720/2007 se regulan previsiones y obligaciones en relación con el encargado del tratamiento en el título II, de principios de la protección de datos, en sus artículos 20, 21 y 22, y en el título VIII, artículos 82 y 88 se contemplan las garantías de seguridad que deberá cumplir el encargado del tratamiento de conformidad con el artículo 12 de la Ley15/1999.

El artículo 20. 2 que cita el consultante introduce un poder de supervisión sobre el encargado que se traduce en que el responsable del fichero o tratamiento estará legitimado para realizar controles durante el período de vigencia del contrato para verificar el cumplimiento de las medidas

de seguridad establecidas y adoptar las medidas correctoras oportunas. Entre estas medidas, se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a datos de carácter personal. Disponer de este documento de seguridad es una obligación para todos los responsables de ficheros y, en su caso, para los encargados del tratamiento, con independencia del nivel de seguridad que sea necesario aplicar, que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente de acuerdo con lo dispuesto en el artículo 88 del Reglamento que regula su contenido.

El artículo 88. 5 establece que "Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado, con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo." En su número 6 determina que "En los casos en los que los datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento."

"El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados, que puedan influir en el cumplimiento de las medidas de seguridad implantadas." Según reza el número 7 del mismo artículo. Este documento ha de especificar los procedimientos y controles periódicos a realizar para verificar el cumplimiento por el encargado del tratamiento de lo dispuesto por el propio documento, lo que el responsable puede hacer constar como cláusula del contrato entre ambos y en las instrucciones que señale al encargado al respecto.

Las medidas de seguridad adoptadas por el encargado del tratamiento deberán plasmarse en un documento de seguridad distinto al que haya de realizarse por el responsable del fichero o tratamiento, dado que los extremos a incluir en el documento se referirán a las actividades desarrolladas por el encargado del tratamiento, no coincidiendo éstas en la mayor parte de los casos con las que realice el responsable.

III

El Reglamento clasifica las medidas de seguridad que deberán implementarse y especificarse en el documento de seguridad en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información (artículos 80 a 114).

Cualquier operación de tratamiento realizada sobre un determinado fichero, una de las cuales sería la atribuida al encargado del tratamiento, deberá someterse a las medidas de seguridad que para ese fichero imponga el Reglamento.

En consecuencia, el hecho de que el encargado del tratamiento pudiera acceder, aunque fuera de manera excepcional o puntualmente, a datos a los que por aplicación del Reglamento les resulte de aplicación las medidas de seguridad de nivel medio o alto, ello implicaría que aquél deberá cumplir con las exigencia que para este tipo de datos dispone el Reglamento, incluido su reflejo en el documento de seguridad.

A partir del nivel medio y alto de medidas de seguridad, el Reglamento exige que en el documento de seguridad se designe el responsable de seguridad artículos (95 y109) encargado de coordinar y del control periódico de las medidas definidas en el documento y que, en ningún caso, supone una exoneración de las responsabilidades en que puedan incurrir tanto el encargado como el responsable del tratamiento. No parece ilógico concluir que el responsable de seguridad pueda verificar que el encargado del tratamiento cumple con las estipulaciones del contrato del artículo 12 de la Ley y comunique los incumplimientos posibles al responsable posibilitando que éste vigile o vele por que el encargado cumpla las garantías de la protección de datos, es decir, que cumpla de buena fe con las obligaciones nacidas del contrato o negocio jurídico suscrito, como establece el artículo 1258 del Código Civil para todos los contratos.

IV

Así mismo, el artículo 96. 1 del Reglamento exige que los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se sometan, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título VIII. Su realización es obligatoria para ficheros de nivel medio y alto, al menos cada dos años y, excepcionalmente, si se han realizado modificaciones sustanciales en el sistema de información, deberá realizarse una auditoría para comprobar la adecuación, adaptación y eficacia de las medidas de seguridad. El informe que resulte de la auditoría deberá pronunciarse sobre tales extremos y las recomendaciones propuestas, que deberán ser analizados por el responsable

de seguridad, que las elevará, a su vez, al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas.

Por último, señala su número 3 que dicho Informe quedará a disposición de la Agencia Española de Protección de Datos, lo que convierte al mismo en un soporte de información respecto al cumplimiento de la normativa sobre protección de datos por parte tanto del responsable como del encargado de los tratamientos.

Todo ello en aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal,