Informe 0021/2009

La consulta plantea dudas respecto a la utilización de las claves de acceso a los equipos informáticos de la consultante por parte de los trabajadores de la empresa TRAGSA.S.A con la que la consultante tiene contratada la prestación de servicios de sus empleados en las dependencias del organismo público consultante, de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y en el Real Decreto 1720/2007, de 21 de diciembre, que aprueba el Reglamento de dicha Ley.

I

En el caso consultado la empresa cuyos trabajadores prestan sus servicios en las dependencias administrativas del organismo público consultante, realizando tareas en la tramitación de diversos tipos de expedientes administrativos, estaría tratando y accediendo a datos de carácter personal por cuenta de terceros, esto es, estaríamos ante la figura del encargado de tratamiento contemplada en el artículo 3.g) de la LOPD que la define como “la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.”

Como señala la Sentencia de la Audiencia Nacional de 20 de septiembre de 2002 (JUR/2003/49995), “existe encargo de tratamiento cuando la transmisión o cesión de los datos está amparada en la prestación de un servicio que el responsable del tratamiento recibe de una empresa externa o ajena a su propia organización, y que le ayuda en el cumplimiento de la finalidad del tratamiento de datos consentida por el afectado.”

En todo caso, sería de aplicación a la empresa tercera el régimen establecido en el artículo 12 de la Ley Orgánica 15/1999 y en el Capítulo III del Título II del Reglamento que la desarrolla, caracterizado por las siguientes especialidades:

a) En primer lugar, será preciso que la actuación del encargado del tratamiento se limite a la prestación de los servicios objeto de la contratación. A tal efecto dispone el artículo 20.1 del Reglamento de desarrollo de la Ley

Orgánica 15/1999 que “se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado”.

b) En lo que atañe a los requisitos formales, el artículo 12.2 de la Ley Orgánica impone 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”.

c) Por lo que respecta al periodo de conservación de los datos, el artículo 12.3 establece 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 del tratamiento”.

Añade el artículo 20.3 del Reglamento 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 hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo”. El artículo 22.1 reitera esta previsión, al indicar que “una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento”.

d) Por otra parte, a fin de preservar los derechos del encargado frente a posibles responsabilidades derivadas de su actuación, dispone el artículo 22.1 del Reglamento que “el encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento”.

e) En lo referente a la posible subcontratación de los servicios prestados, el artículo 21 del Reglamento permite esta posibilidad en caso de que el responsable del fichero apodere al encargado para la celebración del segundo contrato en nombre de aquél o cuando se den los requisitos especificados en el apartado 2 del citado precepto:

- “Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar”. SI dicha circunstancia no se hubiera previsto en el contrato, deberá procederse a su modificación posterior, conforme al artículo 22.3. Igualmente, en caso de que en el contrato no conste la

identificación de la empresa subcontratista "será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación".

- "Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero".

- Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato previsto en el artículo 12 de la Ley Orgánica.

f) En cuanto a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica, detallando el artículo 82 del Reglamento el modo en que deberán implantarse las medidas.

g) Por último, según el artículo 12.4, "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", siendo, en consecuencia, de aplicación el régimen sancionador establecido en los artículos 43 y siguientes de la Ley, sujetando el primero de ellos al encargado del tratamiento a dicho régimen".

II

La cuestión concreta planteada en la consulta afecta a la seguridad y confidencialidad de dicho tratamiento de datos de carácter personal. La seguridad de los datos aparece regulada en el artículo 9 de la Ley Orgánica 15/1999 en el siguiente sentido: "1.-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.

2.-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.

3.- Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley."

Las medidas de seguridad se encuentran reguladas en el Título VIII del Real Decreto 1720/2007, que lleva por rúbrica "De las medidas de seguridad en el tratamiento de datos de carácter personal" y el Capítulo I dedicado a las Disposiciones generales se contemplan el alcance, los niveles de seguridad y la aplicación de los mismos. Así el artículo 79 establece que "Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento." Por otro lado el artículo 80 determina que "Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto."

A su vez, el artículo 82.1 establece que "Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado del tratamiento que preste sus servicios en los locales del primero, deberá hacer constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

En cuanto al control de accesos a los equipos informáticos, el artículo 91 señala que: "1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación autorizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio."

Y el artículo 93 señala: "Identificación y autenticación.-1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel

usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

Para el cumplimiento de las medidas de seguridad descritas, es imprescindible que el sistema utilizado para acceder a los datos de los interesados en los expedientes tramitados impida que terceras personas o usuarios no identificados individualmente puedan acceder a la información, como podría suceder en el supuesto planteado en la consulta, que no permite conocer realmente la identidad de los que utilizan la misma clave del administrador o de otros trabajadores usuarios, lo que impide conocer si el acceso a los datos estaba debidamente autorizado y los posibles usos de la información para una finalidad distinta de aquella para la que fueron recabados los mismos, así como determinar las posibles responsabilidades ante una potencial cesión de datos de carácter personal de los afectados que, por imperativo de lo dispuesto en el artículo 11.1 de la Ley Orgánica 15/1999, requeriría el consentimiento de los mismos.

La utilización de claves de acceso, que permitan al interesado tener conocimiento en cada momento de los datos de carácter personal existentes en el fichero resulta sumamente útil, siempre y cuando dicha clave o "dato de control" asegure el carácter personalísimo de la consulta efectuada para conocer la situación concreta a la que se acceda.

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