Informe 0135/2010

La consulta plantea si la creación de un nuevo sistema de videovigilancia, en virtud del cual el cliente puede acceder a las imágenes, del lugar donde se encuentran instaladas las cámaras, incluso de las últimas 48 horas, y cuyo fichero está dado de alta por la entidad consultante, obliga a que el cliente nuevamente de de alta el fichero según la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal.

Según el contenido de la consulta, el cliente si quiere puede acceder a las imágenes, conectándose por control remoto al servidor de la entidad consultante. Por tanto, parece deducirse que el cliente, más que crear su propio fichero, lo que se le permite es acceder al sistema de la empresa de seguridad.

Este simple acceso que efectúa el cliente, encaja en el concepto que de usuario del sistema otorga el Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, en su artículo 2.2 donde se contiene una serie de definiciones aplicables al supuesto de hecho planteado en la consulta;

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Por tanto, usuario es el sujeto y en los términos de la consulta es la persona física que accede al fichero, por otro lado, el perfil de usuario define el tipo de información a la que éste puede acceder y el tipo de acciones que puede realizar.

Por último todo usuario con independencia de su perfil debe de tener un acceso controlado, ese acceso controlado se regula en el 91 del Real Decreto 1720/2007, donde 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 actualizada 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".

En definitiva, no procede que el cliente dé de alta un nuevo fichero. Sin embargo, la entidad consultante sí debe de considerar al cliente como un usuario del sistema, cuyo acceso debe estar regulado en los términos antes señalados y todo ello debe de aparecer reflejado en el documento de seguridad que se encuentra regulado detalladamente en el artículo 88 del citado reglamento, además este control de acceso físico aparece recogido en el artículo 99 del Real Decreto 1720/2007, donde concreta que "Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información".