Informe 0503/2009

La consulta plantea diversas cuestiones relacionadas con el tratamiento de datos de carácter personal realizados por los funcionarios pertenecientes a un determinado departamento de la Consejería de Medioambiente que cita la consultante, en relación con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

I

En primer lugar la consultante se interesa por la inscripción en el Registro General de esta Agencia, del fichero público de denuncias medioambientales que, según manifiesta, fue creado mediante la Orden del Consejero de Medioambiente de 2 de octubre de 2007 en cumplimiento de lo señalado por el artículo 20 de la LOPD y que estaría en funcionamiento. Al respecto, efectuada la consulta pertinente, se señala que el citado fichero no aparece entre los diferentes que sí tiene inscritos la citada Consejería, por lo que ha de recordarse lo señalado en el artículo 39.2 a) de la LOPD que establece la obligación de inscripción en el Registro General de Protección de Datos de los ficheros de que sean titulares las Administraciones Públicas.

Y en el artículo 55 del Real Decreto 1720/2007 que dice: "Notificación de ficheros. 1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de su creación en el diario oficial correspondiente."

La inscripción de dicho fichero podrá efectuarse electrónicamente a través del Sistema Nota obrante en la página web de la Agencia, recordando al propio tiempo, que el incumplimiento de la citada obligación aparece tipificada como infracción en el artículo 43 de la LOPD.

II

La consulta se refiere también a si los funcionarios superiores jerárquicos del órgano administrativo donde se tramitan las denuncias sobre medio ambiente están autorizados a tratar los datos y si tendrían la condición de terceros o usuarios del fichero de denuncias.

Procede aclarar en primer lugar que la Consejería de Medio Ambiente citada ostentaría la condición de responsable del fichero o tratamiento según lo

define el artículo 3 d) de la LOPD : “persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.” Y que la finalidad de dicho fichero sería el ejercicio de potestades de derecho público. Dicho órgano administrativo realiza un tratamiento de datos de carácter personal de las personas físicas afectadas por la denuncia, para lo cual no necesita el consentimiento del afectado, según señala el artículo 6.2 de la LOPD cuando dice: “No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de la Administraciones públicas en el ámbito de sus competencias.”

Por otra parte, los funcionarios adscritos al citado órgano administrativo estarían accediendo y usando los datos personales obrantes en los correspondientes expedientes administrativos en virtud de su relación administrativa o funcionarial con la Consejería de referencia, por lo cual, tampoco precisarían el consentimiento de los afectados titulares de los datos, según señala el mismo artículo 6.2 de la LOPD. Ahora bien, no se consideran encargados del tratamiento las personas físicas, los funcionarios, que tienen acceso a los datos en su condición de empleados dentro de la relación administrativa que mantienen con el responsable del fichero. Dichos funcionarios serían usuarios del fichero.

Por consiguiente, todo tratamiento de datos del fichero de denuncias que se desarrolle por los funcionarios de la citada Consejería para el ejercicio de las competencias que tiene atribuidas la misma sobre la materia, tendrá la legitimación amparada en el artículo 6 citado. No obstante, debe recordarse que los datos de carácter personal objeto de tratamiento, no podrán usarse para finalidades incompatibles, (diferentes) con aquellas para las que los datos hubieran sido recogidos, según señala el artículo 4.2 de la LOPD.

Además, tales funcionarios no podrán considerarse terceros, atendiendo a la definición de tercero que nos da el artículo 5.1 r) del Reglamento, que lo define como “la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento, y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.”

III

Una vez efectuada esta introducción es preciso señalar que el Reglamento de desarrollo de la Ley Orgánica 15/1999, en su Artículo 2.2 contiene una serie de definiciones aplicables al supuesto de hecho planteado en la consulta señalando que, “en particular, en relación con lo dispuesto en el

título VIII de este Reglamento (referido a las medidas de seguridad en el tratamiento de datos de carácter personal) se entenderá por:

a) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

h) Identificación procedimiento de reconocimiento de la identidad de un usuario.

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 y, por último, todo usuario con independencia de su perfil debe de tener un acceso controlado.

El control de acceso, se regula en el artículo 91 del Real Decreto 1720/2007 señalando 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". A su vez, el artículo 91.3.señala que "El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados." Esto es, no se permite la existencia de usuarios y contraseñas compartidas, para lo cual es necesario que cada usuario tenga una identificación de carácter exclusivo y la par que sea secreta, por ello, debe implantarse un procedimiento que garantice la seguridad y confidencialidad en el otorgamiento de identificación y autenticación de los usuarios (esto es, que la contraseña sólo sea conocida por el usuario).

Estos dos requisitos se detallan en el artículo 93 del citado Reglamento señalando que " 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.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible."

Además lo señalado sólo es aplicable respecto de las medidas de seguridad de nivel básico, pero en el tratamiento o acceso a los datos referidos a la salud, como serían los diagnósticos médicos en el fichero de datos de minusválidos a que se refiere el consultante, deberá cumplirse con las de nivel alto, así lo exige el artículo 81.3 "3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: (..)
a) Los que se refieran a datos de ideología, afiliación sindical, religión creencias, origen racial, salud o vida sexual.

En este último caso se debe crear un Registro de accesos, así lo determina el artículo 103 del Real Decreto 1720/2007 donde se determina que "1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.(..)".

El cumplimiento de todas estas medidas deberá de recogerse en el llamado documento de seguridad y que se encuentra regulado detalladamente en el artículo 88 del citado reglamento "1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.