Expediente Nº: E/02964/2014

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas de oficio por la Agencia Española de Protección de Datos ante la DIRECCION GENERAL DE LA GUARDIA CIVIL, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 13 de marzo de 2014, tuvo entrada en esta Agencia un escrito en el que se expone que un Suboficial del cuartel de la Guardia Civil de Puerto Serrano utiliza todos los meses el terminal portátil del sistema de transmisión de información de la Unidad, sistema interno comunicación de la Guardia Civil denominado Sirdee (número del terminal 33140), los números de D.N.I. del padrón municipal así como de otro listado que posee para ir alternando. De dicho padrón municipal tiene una copia, la cual fue cedida para fines como localización de personas para entrega de citaciones judiciales, efectos identificativos en las dependencias cuando los mismos se niegan o para comprobar la veracidad de los datos facilitados.

La introducción de las supuestas personas identificadas, se realiza a través de una sesión en la propia emisora Sirdee, la cual se abre con el D.N.I. de la persona que inicia la sesión, y se hace constar la hora, la fecha y las personas identificadas así como la persona que ha realizado la consulta.

Los supuestos identificados son introducidos uno tras otro de forma continuada, sin tiempo entre dato y dato, lo que evidencia que no es un acto real de identificación si no la utilización de la base de datos referida.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Según manifiestan los representantes de la Dirección General de la Guardia Civil, El sistema SIRDEE (Sistema Integrado de Radiocomunicaciones Digitales de Emergencias del Estado) es una red de comunicaciones seguras móviles de voz y datos del Ministerio del Interior que, entre otras finalidades, permite realizar consultas desde terminales móviles por nombre, apellidos, Documento de Identidad y matricula de vehículos, a los datos obrantes en los ficheros INTPOL, BDSN (Base de Señalamientos Nacionales), N.SIS (Sistema de información Schengen), Registro de Vehículos y Registro de Conductores.

No es por tanto un Sistema de Información. Es una red de comunicación para facilitar al personal de servicio las consultas desde terminales móviles a los ficheros citados.

Los usuarios que tienen acceso a este sistema corresponden especialmente a personal destinado en Unidades Operativas, que prestan Servicios de Seguridad

Ciudadana. La autenticación se realiza mediante usuario y contraseña, según se establece en los respectivos Documentos de Seguridad de los Ficheros.

SIRDEE es totalmente independiente del sistema con SIGO, y los usuarios autorizados a cada uno de ellos pueden ser los mismos o distintos.

El número de consultas realizadas sobre el sistema SIRDEE por el Sargento Comandante de Puesto de Puerto Serrano en Cádiz, durante los meses de enero y febrero de 2014 es de 200, y no están repetidos los DNI consultados.

Según indican los representantes de la Guardia Civil estas consultas no tienen relación con las identificaciones grabadas en SIGO por el usuario referido.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el Director de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

La comunicación de hechos denunciados se concreta en la utilización de los datos del padrón municipal para finalidades incompatibles con las que se deben tratar.

La LOPD además de sentar el principio de consentimiento, regula en su artículo 4 el principio de calidad de datos. El apartado 2 del citado artículo 4, dispone: *"Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos."* Las *"finalidades"* a las que alude este apartado 2 han de ligarse o conectarse siempre con el principio de pertinencia o limitación en la recogida de datos regulado en el artículo 4.1 de la misma Ley. Conforme a dicho precepto los datos sólo podrán tratarse cuando *"sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido."* En consecuencia, si el tratamiento del dato ha de ser "pertinente" al fin perseguido y la finalidad ha de estar "determinada", difícilmente se puede encontrar un uso del dato para una finalidad *"distinta"* sin incurrir en la prohibición del artículo 4.2 aunque emplee el término *"incompatible".*

La citada Sentencia del Tribunal Constitucional 292/2000, se ha pronunciado sobre la vinculación entre el consentimiento y la finalidad para el tratamiento de los datos personales, en los siguientes términos: *"el derecho a consentir la recogida y el tratamiento de los datos personales (Art. 6 LOPD) no implica en modo alguno consentir la cesión de tales datos a terceros, pues constituye una facultad específica que también forma parte del contenido del derecho fundamental a la protección de datos. Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aún cuando puedan ser compatibles con estos (Art. 4.2 LOPD), supone una nueva posesión y uso que requiere el consentimiento del interesado. Una facultad que sólo cabe limitar en atención a derechos y bienes de*

relevancia constitucional y, por tanto, esté justificada, sea proporcionada y, además, se establezca por ley, pues el derecho fundamental a la protección de datos personales no admite otros límites. De otro lado, es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales. Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta. Pues en otro caso sería fácil al responsable del fichero soslayar el consentimiento del interesado mediante la genérica información de que sus datos pueden ser cedidos. De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (Art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia."

La Audiencia Nacional, en diferentes Sentencias, considera que el artículo 4 de la LOPD establece una sutil distinción entre finalidad de la recogida y finalidad del tratamiento, *"pues la recogida sólo puede hacerse con fines determinados, explícitos y legítimos, y el tratamiento posterior no puede hacerse de manera incompatible con dichos fines. Así pues, y de acuerdo con el artículo 1.b) de la Directiva 95/46/CE de 24 de octubre de 1995 (en cuya redacción se inspira el repetido artículo 4.2 de nuestra LOPD), si la recogida se hizo con fines determinados, cualquier uso o tratamiento posterior con finalidad distinta es incompatible con la primera finalidad que determinó la captura por lo que, en este contexto, diferente o incompatible significan lo mismo."*

De lo expuesto cabe concluir que la vigente LOPD ha acentuado las garantías precisas para el tratamiento de los datos personales en lo relativo a los requisitos del consentimiento, de la información previa a éste y de las finalidades para las que los datos pueden ser recabados y tratados.

En definitiva, los datos no pueden ser tratados para fines distintos a los que motivaron su recogida, pues esto supondría un nuevo uso que requiere el consentimiento del interesado.

En el caso presente, la Dirección General de la Guardia Civil ha indicado el uso que se realiza de la red de comunicaciones SIRDEE que es facilitar al personal destinado en Unidades Operativas que prestan servicios de Seguridad Ciudadana, y tras comprobar los accesos del Sargento Comandante de Puerto Serrano, verifican que no se han realizado consultas con DNI repetidos.

Por tanto, tras las actuaciones previas de investigación realizadas, no se ha obtenido acreditación de accesos al sistema SIRDEE con finalidades incompatibles o diferentes para las que se facilita a los usuarios.

Por lo tanto, de acuerdo con lo señalado,

Por el Director de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a la DIRECCION GENERAL GUARDIA CIVIL y al denunciante**.**

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Real Decreto 1720/2007, de 21 diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, los interesados podrán interponer, potestativamente, recurso de reposición ante el Director de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución, o, directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la LJCA, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 del referido texto legal.

José Luis Rodríguez Álvarez
Director de la Agencia Española de Protección de Datos