



Expediente N°: E/01313/2016

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el Ministerio de Defensa, en virtud de denuncia presentada por Don **A.A.A.**, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 15 de febrero de 2016, tuvo entrada en esta Agencia un escrito remitido por Don **A.A.A.**, en el que expone lo siguiente:

Que es militar de la Sección de Honores de la Armada Española, por comisión forzosa, y que el día 4 de febrero de 2016 recibió un correo electrónico del responsable del fichero de la sección solicitándole sus datos de carácter personal, como son nombre, apellidos, DNI y teléfono, pero no hacen alusión a las leyes de protección de datos; pero los facilita.

El mismo día 4 recibió, por correo electrónico, un fichero con los datos personales de todos los integrantes de la sección, en los que se incluyen los del denunciante y son enviados a todos los integrantes de la sección, todo esto sin solicitarle su consentimiento para la difusión de los mismos.

También, le agregan a dos grupos de la aplicación whatsapp alegando la practicidad de los mismos para comunicaciones de dicha sección sin solicitar su consentimiento y difundiendo su número de teléfono a todos los integrantes de dicho grupo.

Se adjunta con el escrito de denuncia correo electrónico remitido desde la dirección <...@fn.mde.es>, el día 4 de febrero de 2016, dirigido a “31” destinatarios cuyas direcciones de correo electrónico son del dominio “mde.es”, a excepción de uno de ellos “gmail.com”, entre los que se encuentra el denunciante <...1@fn.mde.es>, y como Asunto: BASE DE DATOS CORREGIDA. Con el que se adjunta el archivo “***ARCHIVO.1.xlsx”.

En el citado archivo consta información de “34” personas con: nombre, apellidos, NIF, pelotón, destino, RPV, móvil, fecha antigüedad empleo, fecha inicial comisión secc. honores, día concilia y jefe del destino (categoría, nombre y apellidos), entre los que se encuentra el denunciante.

Con fecha de 26 de abril de 2016, el denunciante remite nuevo escrito a la Agencia manifestando que el fichero en el que deberían estar los datos es el denominado: Gestión de personal del OAJ DE JEASER.

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:

1. Se ha verificado por parte de la Inspección de Datos que el titular del dominio <mde.es> es el Ministerio de Defensa de España.

2. El Ministerio de Defensa ha informado a la Agencia, en relación con los hechos comunicados por el denunciante, lo siguiente:

Dentro del plan de comunicación en la Sección de Honores se encuentra el envío del archivo temporal denominado "BASE DE DATOS CORREGIDA", que integra los datos de los militares pertenecientes a la misma con la finalidad de permitir la comunicación, la coordinación y la localización del personal.

El correo se envía a 31 personas, todas ellas pertenecientes a diferentes destinos dentro de la Armada en Madrid, las cuales necesitan estar en contacto permanente para hacer posible su localización si las necesidades del servicio así lo exigen, todo ello cumpliendo la finalidad de gestionar al personal.

Las personas incluidas en el correo enviado pertenecían al personal de la Sección de Honores, teniendo todas ellas suscrito el compromiso de confidencialidad a que hace referencia el artículo 10 de la Ley Orgánica 15/1999, en el que se indica expresamente la obligación de guardar secreto en relación a todos los datos personales que como consecuencia del desempeño de sus tareas tengan conocimiento, así como de adoptar todas las medidas de seguridad necesarias sobre toda la información con datos de carácter personal que manejen en el desarrollo de sus actividades personales. Se adjunta Cláusula de Confidencialidad suscrita por una de las personas receptoras del correo electrónico.

Tanto los datos del fichero adjunto como los datos de las direcciones de correo electrónico, forman parte de dos ficheros responsabilidad de la Armada en la Comunidad de Madrid, en concreto de la Jefatura de Asistencia y Servicios Generales (JEASER). Estos ficheros están inscritos en el Registro General de Protección de Datos, y fueron creados por la Orden DEF/921/2012, de 23 de abril, por la que se crean y suprimen ficheros de datos de carácter personal de diversos órganos de la Armada:

Fichero de gestión de personal del OAJ de JEASER, cuya finalidad es el control del personal destinado en el Órgano Auxiliar de Jefatura (OAJ) de la JEASER así como del personal en situaciones dependientes de JEASER.

Fichero de gestión de personal del Detall de la Ayudantía Mayor del CGA, cuya finalidad es gestión del personal civil y militar de la Ayudantía Mayor del Cuartel General de la Armada para su control y la Gestión de guardias.

Por otra parte, no es necesario que los titulares de los datos (militares) otorguen su consentimiento para el tratamiento de datos de carácter personal. La excepción al consentimiento viene dada por el artículo 23 punto segundo de la Ley Orgánica 9/2011, de 27 de julio, de derechos y deberes de los miembros de las Fuerzas Armadas, en el que se establece que *"El militar tiene la obligación de comunicar en su unidad el lugar de su domicilio habitual o temporal, así como cualquier otro dato de carácter personal que haga posible su localización si las necesidades del servicio lo exigen"*. En este supuesto, y atendiendo a las finalidades antes descritas, el dato de correo electrónico se consideró necesario para poder llevar a cabo su localización.

En el Ministerio de Defensa, como regla general el personal, bien propio o externo, cuenta con una dirección de correo electrónico corporativa, pero el personal de marinería, dependiendo del destino que desempeñen en su puesto de trabajo, no



necesariamente posee una dirección de correo corporativo como es el caso de la dirección <gmail.com>.

También, con la finalidad de permitir una comunicación y coordinación entre los militares, se crea un grupo de whatsapp como un medio más, junto con el teléfono y el correo electrónico, de las "31" personas.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora 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

El artículo 6 de la LOPD, cuya posible vulneración se imputaría al Ministerio de Defensa por tratar los datos del denunciante para enviarle el correo reseñado en los antecedentes, dispone que:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

El tratamiento de datos sin consentimiento constituye un límite al derecho fundamental a la protección de datos. Este derecho, en palabras del Tribunal Constitucional en su Sentencia 292/2000, de 30 de noviembre, (F.J. 7 primer párrafo), *"...consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el estado o un particular (...)"*.

Son pues elementos característicos del derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y tratamiento de sus datos personales y a saber de los mismos.

La LOPD además de sentar el anterior 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 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.

III

Tras las actuaciones previas de investigación realizadas se ha tenido conocimiento de lo siguiente:

El denunciante, en el momento de recibir el correo denunciado, 4 de febrero de 2016, con los datos de todos sus compañeros de la Sección de Honores de la Armada Española, era miembro de dicha Sección. Las personas a las que se facilita el listado con datos personales de sus compañeros son los miembros de la Sección de Honores, con la finalidad de estar en contacto permanente y poder localizarles si las necesidades del servicio lo exigen.

En consecuencia, no sería necesario el consentimiento al unirles a todos una relación laboral con el Ministerio de Defensa, estando recogido de forma expresa en el artículo 23 punto segundo de la Ley Orgánica 9/2011, de 27 de julio, de derechos y deberes de los miembros de las Fuerzas Armadas, en el que se establece que *"El militar tiene la obligación de comunicar en su unidad el lugar de su domicilio habitual o temporal, así como cualquier otro dato de carácter personal que haga posible su localización si las necesidades del servicio lo exigen"*.

En cuanto a la finalidad para la que se les facilita el listado de compañeros de la Unidad es permitir la comunicación, la coordinación y la localización del personal; es decir, es adecuada con la relación laboral que les une. No obstante, podría revisarse la información que se facilita a los miembros de la Sección de Honores por si alguno de los apartados no fuese necesario, de acuerdo con el principio de minimización de datos: adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Por último, el artículo 10 de la LOPD establece que *"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo"*.

Es preciso tener en consideración la Sentencia de 14 de abril de 2008 de la Audiencia Nacional, que resolvió el recurso 379/2006 planteado contra una resolución de esta Agencia. En su Fundamento de Derecho Sexto recoge lo siguiente: *<Precisamente el artículo 11.2.c) de la LOPD establece entre sus excepciones a la necesidad del consentimiento para poder facilitar datos a un tercero "que el tratamiento responda a una libre y legítima aceptación de una relación jurídica cuyo desarrollo cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros". Ciertamente el denunciante está integrado en la asociación sancionada en cuanto propietario de una parcela sita en la urbanización [...] y en el seno de esa relación asociativa es legítimo facilitar información a los asociados sobre cuestiones de interés común, vinculadas a su actividad [...] Por tanto, la comunicación del nombre y apellidos de quien había presentado la denuncia, que también era*



asociado, en ámbito limitado de los miembros de la asociación no supone una revelación de secreto que deba ser sancionada al no existir deber de confidencialidad en este caso por estar amparada la comunicación en la relación jurídica asociativa>.

En el presente caso, según se desprende de la documentación aportada por el afectado, existe una relación laboral que vincula a los destinatarios del correo, existiendo constancia, asimismo, que todos ellos han suscrito el compromiso de confidencialidad a que hace referencia el mencionado artículo 10 de la LOPD.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución al MINISTERIO DE DEFENSA y a Don **A.A.A..**

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD, 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 Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora 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.

Mar España Martí
Directora de la Agencia Española de Protección de Datos