Expediente Nº: E/03949/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la ***DIRECCION GENERAL GUARDIA CIVIL,*** en virtud de denuncia presentada por D. ***A.A.A.*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 7 de junio de 2013, tuvo entrada en esta Agencia escrito de D ***A.A.A.***, como Secretario General Provincial de la Asociación Unificada de Guardias Civiles (AUGC) en la Provincia de Huelva, en el que denuncia que en el acuartelamiento de la Comandancia de la Guardia Civil de Huelva, existe un buzón en el que se introduce la correspondencia que se remite a la AUGC y han recibido, de forma anónima, dos "Pen-Drive" (Lápices de memoria) que según se informa en el documento con el que se reciben sin firma y sin ningún tipo de identificación, del que aportan copia, pertenecen al ***EMPLEO.1 de la Guardia Civil, ***CARGO.1 de la Unidad de Seguridad Ciudadana de la Comandancia de Huelva, D. ***B.B.B.***.

Así mismo, en el citado documento informan a la AUGC de que en los "Pen-Drive", se encuentran almacenados documentos relacionados con componentes de la Guardia Civil que no están a las órdenes del mencionado ***CARGO.1 de la Unidad de Seguridad Ciudadana y que en algunos casos son documentos confidenciales en los que no ha participado ni debería tener conocimiento, por lo que consideran que dichos documentos han sido entregados por los responsables de su confección de forma indebida u obtenidos de forma irregular.

La AUGC manifiesta que no desea tener acceso a los documentos que pudieran encontrarse en los "Pen-Drive" por lo que los remiten a esta Agencia con objeto de que se valore la responsabilidad que se estime oportuna.

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:

A) En las presentes actuaciones, se accede a los dos "Pen-drive", remitidos con la denuncia comprobando que:

1. Uno de ellos contiene múltiple documentación relativa tanto a miembros de la Guardia Civil como a ciudadanos, así como modelos de tramitación y solicitudes correspondientes a la Guardia Civil, algunos de los documentos figuran firmados por ***B.B.B..*** Se observa que por la cantidad de información que contiene podría tratarse de una copia del disco duro de un ordenador.
2. Respecto al otro Pen-drive, no se ha podido examinar su contenido, ya que al intentar acceder al mismo, da un mensaje de error.

B) Con fecha 23 de diciembre de 2013, se da traslado de la denuncia y de una muestra del contenido de uno de los Pen-drive a la Dirección General de la Guardia Civil, con

objeto de que realicen las actuaciones necesarias para emitir un informe a la Agencia en relación con los hechos denunciados.

Con fecha 10 de enero de 2014, se recibe en esta Agencia un correo electrónico de D. ***B.B.B.***, en el que manifiesta que:

1. Ha tenido conocimiento de que la AUGC han remitido a esta Agencia dos "Pen-drive" que pudieran ser de su propiedad y que este hecho ha dado lugar al inicio de las presentes actuaciones.
2. Según manifiesta, desde primeros del año 2013, aproximadamente, dos Pen Drive que contenían archivos suyos privados relacionados con su vida personal y su trabajo, desaparecieron de su puesto de trabajo.
3. Que dichos dispositivos de memoria fueron sustraídos con un fin determinado, para interponer una denuncia contra él.
4. Que se pone a disposición de esta Agencia para identificar los sistemas de almacenamiento y para verificar el contenido de los mismos, solicitando la devolución de ellos si fuera posible y se estima conveniente.

C) Con fecha 12 de febrero de 2014, la Dirección General de La Guardia Civil ha remitido a esta Agencia un informe en relación con los hechos denunciados en el que se pone de manifiesto lo siguiente:

1. De la documentación aportada y de las averiguaciones hasta la fecha practicadas, resulta que los lápices de memoria sobre los que versa la información solicitada le fueron sustraídos al ***EMPLEO.1 D. ***B.B.B.*** de su despacho oficial en la Comandancia de Huelva, significando que dicha dependencia se encuentra dotada de cerradura con llave, siendo la causa probable las conflictivas relaciones que mantiene con algunos subordinados por cuestiones profesionales, por lo que desde que el citado ***EMPLEO.1 ha tenido noticia de la sustracción, ha dado cuenta de la misma a sus superiores, formulando además la correspondiente denuncia, sin que hasta la fecha, el autor o autores hayan podido ser identificados.
2. De la muestra de documentos que se adjuntan a la denuncia remitida, el firmante de algunos de ellos es el propio interesado, en unos con su actual empleo de ***EMPLEO.1 y en otros con el de ***EMPLEO.2 que antes ostentaba. Los demás, están referidos a trámites administrativos, como es la solicitud de aprobación previa de presupuesto para traslado de mobiliario, y a, diversas actuaciones profesionales que le pueden servir de modelo en el ejercicio de sus funciones.
3. A este respecto, señalan que la Guardia Civil ha aprobado, instaurado, y llevado a la práctica, no sólo todas las medidas a las que viene obligada de conformidad con la normativa vigente en materia de protección de datos personales, sino además aquellas otras que ha estimado pertinentes para incrementar la seguridad de sus ficheros al nivel que ha estimado adecuado al tipo de información sensible que maneja, desarrollando paralelamente actividades de coordinación, seguimiento y control de la efectiva aplicación de tales medidas, tanto a nivel interno en cada uno de los ficheros de la Guardia Civil por sus propios responsables, tal y como marca la normativa, sino además a nivel institucional, mediante la creación de departamentos especializados en los que se desarrolla un seguimiento continuado y control

de los tratamientos que se llevan a efecto en los diferentes ficheros dependientes de la Institución para asegurar el máximo rigor en el cumplimiento de todas las medidas adoptadas en materia de Seguridad de la Información, garantizando de esta forma la debida observancia de la citada obligación de resultado que impone el artículo 9 de la LOPD.

4. En este caso, la seguridad de los datos incorporados a los lápices de memoria, o al menos al que se ha podido abrir, ha estado en todo momento garantizada mientras ha permanecido en poder del ***EMPLEO.1 B.B.B., pues además de las medidas que tienen los equipos informáticos de su Unidad, el acceso a su despacho se encuentra restringido, y dotado de cerradura de la que, en principio, únicamente dispone de llave su adjudicatario. Además, dicha dependencia se encuentra a su vez en dependencias oficiales a las que solamente tienen acceso personal del Cuerpo de la Guardia Civil, teniendo todos ellos la responsabilidad de asegurar que las aplicaciones, recursos informáticos y los datos propios de la Institución sean usados únicamente para el desarrollo de la operativa propia para la que fueron creados o implantados y sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales o que infrinjan los derechos de la Guardia Civil o de terceros.

5. Por otra parte, los miembros del Cuerpo deben abstenerse en toda situación de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros la información contenida en los sistemas informáticos, sin que ninguna de dichas acciones haya sido llevada a cabo por el ***EMPLEO.1 denunciado, que ha sido objeto de la sustracción de dos lápices de memoria que poseía con información que le resulta de utilidad para las labores que tiene que desempeñar.

6. Las referidas medidas figuran entre las Normas Básicas de Seguridad implantadas en esta Institución, que resultan de aplicación a todas las Unidades de la Guardia Civil, incluida la del puesto de trabajo del denunciado, de las que aportan copia.

7. Además, señalan que la información contenida en las memorias USB sustraídas, según ha sido referida, se corresponde con el desarrollo de competencias legalmente atribuidas a la Guardia Civil, en cuyo desarrollo diario se comprende la utilización de modelos que faciliten a los agentes la instrucción de las respectivas diligencias policiales o administrativas en la que participen en cada caso. Consideran que esta forma de actuar no constituye infracción alguna cuando, como aquí ocurre, por parte del usuario autorizado se mantiene dicha información dentro del fichero en el que se enmarca el tratamiento de los datos.

8. Por tales motivos en ningún momento aprecian infracción alguna de tales medidas en la actuación llevada a cabo por parte del ***EMPLEO.1 denunciado, en tanto que por parte del mismo en ningún momento se ha producido ninguna salida de información personal del fichero fuera del ámbito del mismo, pues los citados soportes se encontraban, como hemos señalado, en su puesto de trabajo que, insisten, se encuentra dotado de todas las medidas de seguridad que resultan exigibles.

9. A este respecto conviene destacar las disposiciones 23 a 26 de las citadas Normas que figuran en el documento que aportan, contenidas en el epígrafe

2.3 “Salidas de información” de cuya virtualidad resulta que la Guardia Civil ha dado instrucciones precisas para que cualquier salida de información del ámbito del fichero se lleve a efecto sólo si previamente se cuenta con la previa autorización del responsable del tratamiento y, como sería aquí el caso, cifrando la información. Tales preceptos no han sido infringidos en ningún momento pues ningún dato de carácter personal ha sido sacado del fichero por usuario autorizado, sino que la información se contenía en el ámbito propio del mismo.

10. Según manifiestan, cosa distinta es que la salida de información del fichero se produzca, tal y como aquí ha ocurrido, como consecuencia de la sustracción de los citados soportes de su legítima ubicación dentro del ámbito del fichero, con lo que nos encontramos ante una actividad no amparada por ordenamiento jurídico, y en tal sentido, ilegal, susceptible incluso de encajar en algún tipo penal, llevada a efecto por un tercero, con toda probabilidad otro miembro de la Guardia Civil que, aprovechándose de tal circunstancia, y de la posibilidad que la misma le ofrece para acceder a dependencias oficiales, ha procedido de esta forma con la intención de perjudicar al ***EMPLEO.1, por lo que, de tales circunstancias, en ningún momento pueden imputarse responsabilidad a la Institución o a dicho ***EMPLEO.1, pues en todo momento ha actuado de manera diligente, formulando además la correspondiente denuncia penal, pues de lo contrario se estaría vulnerando el principio de culpabilidad.

11. De todo cuanto antecede, y una vez realizadas las actuaciones necesarias para emitir el informe interesado por esa Agencia, resultan las siguientes CONCLUSIONES:

    a. Los lápices de memoria sobre los que versa la solicitud de la información formulada por esta Agencia le fueron sustraídos al ***EMPLEO.1 B.B.B. de su despacho oficial en la Comandancia de Huelva, encontrándose el mismo dotado de cerradura con llave y en dependencias oficiales a las que únicamente tienen acceso personal del Cuerpo de la Guardia Civil.

    b. La información contenida en los lápices de memoria se corresponde con modelos o formularios para el desarrollo de competencias legalmente atribuidas a la Guardia Civil, manteniéndose la misma según el punto anterior, y por parte de usuario que cuenta con autorización, dentro del fichero en el que se enmarca el tratamiento con datos personales que se ha visto afectado, sin que en ningún momento se haya realizado cesión o difusión alguna de la misma, ni por parte de dicho usuario, ni por esta Institución, teniendo en cuenta en este sentido que los datos se ha obtenido de manera ilícita y han sido comunicados de forma anónima.

    c. Desde que el citado ***EMPLEO.1 ha tenido noticia de la citada sustracción ha dado cuenta de la misma a nivel interno, formulando además la correspondiente denuncia penal, sin que hasta la fecha el autor o autores hayan podido ser identificados.

    d. Por parte de esta Institución se han aprobado, instaurado, y llevado a la práctica más medidas de aquellas a las que viene obligada de conformidad con la normativa vigente en materia de protección de

datos de carácter personal, desarrollando además actividades de coordinación, seguimiento y control de la efectiva aplicación de tales medidas, tanto por los respectivos responsables de cada uno de sus ficheros como por departamentos especializados creados a tal fin, todo ello para asegurar el máximo rigor en el cumplimiento del deber de seguridad que establece el artículo 9 de la LOPD, lo que no obsta sin embargo a que se puedan producir actuaciones presuntamente delictivas, tal y como aquí ha ocurrido y ha sido objeto de la correspondiente denuncia, de las que en ningún momento pueden imputarse responsabilidades a esta Institución o a dicho ***EMPLEO.1, pues de lo contrario se estaría vulnerando el principio de culpabilidad.

12. En relación con la desaparición de los dispositivos de memoria, ***B.B.B.***, ha remitido a esta Agencia mediante correo electrónico de fecha 13 de mayo de 2014, copia de la denuncia que interpuso ante la Policía Judicial de Huelva (Comandancia de la Guardia Civil), con fecha 29 de enero de 2014, en la que pone de manifiesto la desaparición a primeros del año 2013, en su despacho oficial, no compartido, en las dependencias de la Guardia Civil, de dos pen-drives de memoria, conteniendo múltiples archivos relacionados con su vida y con su trabajo.

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

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."

El deber de confidencialidad obliga no sólo al responsable del fichero sino a todo aquel que intervenga en cualquier fase del tratamiento.

Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Así el Tribunal Superior de Justicia de Madrid ha declarado en su Sentencia de 19 de julio de 2001: "*El deber de guardar secreto del artículo 10 queda definido por el carácter personal del dato integrado en el fichero, de cuyo secreto sólo tiene facultad de disposición el sujeto afectado, pues no en vano el derecho a la intimidad es un derecho individual y no colectivo. Por ello es igualmente ilícita la comunicación a cualquier tercero, con independencia de la relación que mantenga con él la persona a que se refiera la información (...)".*

En este sentido, la sentencia de la Audiencia Nacional de fecha 18 de enero de 2002, recoge en su Fundamento de Derecho Segundo, y tercer párrafo: "*El deber de secreto profesional que incumbe a los responsables de ficheros automatizados, recogido en el artículo 10 de la Ley Orgánica 15/1999, comporta que el responsable –en este caso, la entidad bancaria recurrente- de los datos almacenados –en este caso, los asociados a la denunciante- no puede revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo" (artículo 10 citado). Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la STC 292/2000, y por lo que ahora interesa, comporta que los datos tratados automatizadamente, como el teléfono de contacto, no pueden ser conocidos por ninguna persona o entidad, pues en eso consiste precisamente el secreto.*

Este deber de sigilo resulta esencial en las sociedades actuales cada vez mas complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la CE. En efecto, este precepto contiene un "instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos" (STC 292/2000). Este derecho fundamental a la protección de los datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino" (STC 292/2000) que impida que se produzcan situaciones atentatorias con la dignidad de la persona, "es decir, el poder de resguardar su vida privada de una publicidad no querida"

En el caso que nos ocupa, la Dirección General de la Guardia Civil y quienes intervengan en cualquier fase del tratamiento profesional (el ***EMPLEO.1 de la Comandancia de la Guardia Civil en Huelva) son responsable del fichero con datos personales del personal así como de la custodia de la documentación relativa a los mismos y, en el presente caso, determinados documentos relativos a miembros de la institución aparecieron en la AUGC incluidos en dos los lápices de memoria, conducta que, en principio, supone la existencia de un incumplimiento del *"deber de secreto"* , al producirse una ausencia de confidencialidad, por lo que se considera que se ha podido incurrir en una infracción del transcrito artículo 10 de la LOPD.

Por su parte, el artículo 9 de la LOPD establece:

"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."

En el Título VIII del Reglamento de desarrollo de la LOPD, aprobado mediante Real Decreto 1720/2007, de 21 de diciembre, se detallan los requisitos de seguridad que han de reunir los ficheros y tratamientos de datos de carácter personal, en función de la tipología de los datos involucrados.

En el presente caso, de acuerdo con la información y documentación facilitada a la Inspección de Datos obrante al expediente, la salida de los lápices de memoria comprensivos de información personal y de documentación de la Comandancia de Huelva de la Guardia Civil no se ha comprobado fuese debida a falta de medidas de seguridad sino debido al "robo" de aquellos del despacho del ***EMPLEO.1 de la Comandancia de Huelva, D. ***B.B.B.,*** dotado de cerradura con llave, que comunicó a las instancias correspondientes.

III

Respecto a la infracción al *"deber de secreto"* está acreditado que la información de uno de los pen-drive no se pudo acceder al dar "error" y el segundo incluye información sobre documentación de la Comandancia de Huelva (documentos con datos personales de miembros de la Comandancia) y particular del denunciante (fotografías familiares) resultando que no se ha comprobado se haya producido una revelación a terceros dado que la destinataria de los lápices de memoria fue el depósito anónimo en el buzón de correos de la AUGC y ésta afirma haberlos puesto a disposición de esta Agencia sin acceder a los mismos.

La Audiencia Nacional tiene establecida la necesidad de que se produzca una efectiva revelación para que se cometa la infracción i del *"deber de secreto"* y sobre la exigencia de que se produzca revelación efectiva, parte de la necesidad de que aunque se cometa una determinada conducta que pudiera dar lugar a la revelación de secretos, si está, efectivamente no se produce, no es posible sancionar por la revelación de secretos. En la Sentencia correspondiente al recurso 500/2008 se recoge la doctrina sobre esta cuestión exponiendo (el supuesto era el de una remisión de correspondencia

en sobre con ventanilla transparente que permiten ver parte del contenido) que lo relevante es que se haya producido efectiva revelación de datos y que si dicha revelación no se ha producido, no existe infracción. En forma parecida, las sentencias dictadas en el recurso 395/2007 y aquellas que cita (recursos 295/2006 y 377/2005) no permiten entender que se produzca revelación de secretos por la simple remisión de documentación a la persona distinta de la interesada si no se ha acreditado que se haya producido efectiva revelación de datos.

En la sentencia correspondiente al recurso 205/2008 se dijo que *"aunque, es cierto que la documentación no estuvo correctamente custodiada y no era razonable que las historias clínicas viajaran en un camión con el resto de escombros de la demolición de un hotel, la realidad es que ninguna violación del secreto se ha producido y nadie ha llegado a tener noticia de la documentación clínica que, al parecer, sigue custodiada en las cajas en cuestión cuya fotografía ha aportado la parte recurrente"*.

En el caso presente resulta acreditado que la documentación estaba debidamente custodiada dentro del despacho dotado de cerradura con llave del ***EMPLEO.1 ***CARGO.1 de la Comandancia de Huelva y, en el hipotético supuesto no probado, de que alguien tuviera conocimiento de datos reservados, es porque se violentaron las medidas de seguridad establecidas en la Comandancia mediante el acceso al despacho donde estaba depositada la documentación en relación a la que había *"deber de secreto" .*

Por lo tanto, no se considera correcto sancionar por la infracción del *"deber de secreto"* cuando la revelación solo se ha debido a la propia conducta activa del autor/res del robo y dicha conducta ha sido la que ha provocado la revelación.

IV

En cuanto a una supuesta infracción de las *"medidas de seguridad",* el articulo 44.3.h de la LOPD considera infracción grave el mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

En relación a las medidas de seguridad, la SAN de 17/12/2009, recurso 00082/2009, es del criterio que debe aplicarse el mismo razonamiento que es utilizado en relación a la infracción del *"deber de secreto"*, pues en el caso analizado no se puede concluir que las medidas razonables de seguridad no estaban implantadas en la Comandancia de la Guardia Civil de Huelva, puesto que se insiste, los lápices de memoria estaban custodiados en un despacho dotado de cerradura con llave del ***CARGO.1 de la Comandancia y fue necesario el empleo de la conducta activa del autor /es de la sustracción para hacer desaparecer esas medidas de seguridad razonablemente implantadas. En este sentido, la referida SAN de 17/12/2009, es del siguiente tenor: *" Considera esta Sala que la propia conducta activa de los denunciantes eliminando las barreras de seguridad implantadas por la empresa recurrente justifica que se deje sin efecto la sanción frente a la que se recurre y ello pues no se ha acreditado que hubiera omisión de medidas para impedir la recuperación y reutilización de la documentación custodiada. Por último es necesario hacer una simple mención al hecho de que la resolución de la Agencia no considera que hubiera ninguna otra infracción de medidas de seguridad por lo que debe entenderse que el resto de*

exigencias derivadas de la aplicación del R.D. 994/99 habían sido suficientemente cumplimentadas por la empresa recurrente".

Asimismo, procede tener en consideración la SAN de la Sala de lo Contencioso-Administrativo, de fecha 25 de febrero de 2010, que en relación con un caso similar de violentación de las medidas de seguridad , señala lo siguiente:

"En el caso de autos, el resultado es consecuencia de una actividad de intrusión, no amparada por el ordenamiento jurídico y en tal sentido ilegal, de un tercero con altos conocimientos técnicos informáticos que rompiendo los sistemas de seguridad establecidos accede a la base de datos de usuarios registrados en www.....,, descargándose una copia de la misma. Y tales hechos, no pueden imputarse a la entidad recurrente pues, de otra forma, se vulneraría el principio de culpabilidad.

El principio de culpabilidad, previsto en el artículo 130.1 de la Ley 30/1992, dispone que solo pueden ser sancionadas por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia. Esta simple inobservancia no puede ser entendida como la admisión en el derecho administrativo sancionador de la responsabilidad objetiva, que está proscrita después de la STC 76/1999, que señaló que los principios del ámbito del derecho penal son aplicables, con ciertos matices, en el ámbito del derecho administrativo sancionador, requiriéndose la existencia de dolo o culpa. En esta línea la STC 246/1999, de 19 de diciembre (RTC 1991/246), señaló que la culpabilidad constituye un principio básico del Derecho administrativo sancionador. Culpabilidad, que no concurre en la conducta analizada de Portal Latino".

Además, señalar que el ***EMPLEO.1 de la Comandancia de Huelva puso verbalmente en conocimiento de sus superiores la desaparición de los lápices de memoria en el momento de que lo detectó, así como formuló la correspondiente denuncia ante la Policía Judicial de Huelva (Comandancia de la Guardia Civil) con fecha 29 de enero de 2014 cuando tuvo conocimiento de los hechos denunciados ante esta Agencia por la AUGC..

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución a la ***DIRECCION GENERAL GUARDIA CIVIL,*** *D.* ***B.B.B.*** y a D. ***A.A.A..***

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