Procedimiento Nº AP/00081/2009

RESOLUCIÓN: R/01633/2010

En el procedimiento de Declaración de Infracción de Administraciones Públicas **AP/00081/2009**, instruido por la Agencia Española de Protección de Datos a la ***DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL (CUERPO NACIONAL DE POLICÍA)***, vista la denuncia presentada por ***D. A.A.A.*** en representación de D. ***B.B.B.***, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha 13 de marzo de 2009, tuvo entrada en esta Agencia Española de Protección de Datos escrito de D. ***A.A.A.***, en representación de ***D. B.B.B.***, contra la ***DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL (CUERPO NACIONAL DE POLICÍA)***, en el que manifiesta que:

En el mes de febrero de 2009, como consecuencia de la instrucción de diligencias previas por el Juzgado de Instrucción nº 0A de .... se acordó la detención del denunciante por su presunta participación en los hechos allí enjuiciados. Dicha detención se llevó a cabo por los Cuerpos y Fuerzas de Seguridad del Estado elaborándose la correspondiente ficha policial del denunciante con datos personales del mismo, tales como nombre, apellidos, domicilio, D.N.I., filiación, fecha de nacimiento, huellas digitales y fotografías.

El 12 de marzo de 2009 salieron publicadas en varios medios de comunicación nacionales, entre otros: Diario El Mundo, elmundo. es y Veo Televisión, S.A., fotografías del denunciante que se corresponden con las tomadas en dependencias policiales.

Adjunto a la denuncia, se aportaron fotocopias de las fotografías publicadas en los medios de comunicación antes citados.

SEGUNDO: A la vista de los hechos denunciados, en fase de actuaciones previas, por los Servicios de Inspección de esta Agencia se solicita información al organismo denunciado, teniendo conocimiento de que:

1. Con fecha 14 de septiembre de 2009 se realiza inspección en la Unidad de Documentación de Españoles y Archivo del organismo denunciado, constatándose los siguientes extremos:
   a) Esta Unidad se encuentra adscrita a la Subdirección General de Gestión Económica, Técnica y Documental del Cuerpo Nacional de Policía.
   b) Con motivo de la publicación en varios medios de comunicación, de fotografías del denunciante coincidentes con las de su reseña policial, esta Unidad elaboró, con fecha 13 de marzo de 2009, una nota informativa en la que se recogía el resultado de las averiguaciones practicadas por el personal de la Unidad, con objeto de determinar la procedencia de las fotografías publicadas.
   c) De las averiguaciones que se practicaron, se concluye:

- Las fotografías publicadas en los medios de comunicación correspondían a D. B.B.B..
- Las fotografías coincidían con las reseñas que figuraban en el fichero PERPOL, siendo también coincidente el número **** que figuraba en la reseña policial y en las fotografías cuya publicación se denuncia.
- Consultada la aplicación de CONTROL DE ACCESOS DE USUARIOS (CAUPOL) del fichero PERPOL se determinó que se habían producido siete accesos en el período comprendido del 11 de febrero al 4 de marzo de 2009.

d) La Unidad de Documentación de Españoles y Archivo dio traslado de dicha nota informativa a la Dirección Adjunta Operativa. Con posterioridad ha tenido conocimiento de que dos de los accesos realizados por un policía destinado en la Brigada Local de Seguridad Ciudadana de la Comisaría Local de (.....) (Madrid) no estaban suficientemente justificados. Por ello, la Unidad de Asuntos Internos inició actuaciones, cuyo resultado ha sido la tramitación del correspondiente atestado dando cuenta a la autoridad judicial competente.

e) Entre las medidas de seguridad implantadas en el fichero PERPOL, se encuentran las siguientes:

- Existe un procedimiento de alta de usuarios, según el cual la Unidad sólo facilita el acceso al fichero a aquellos usuarios que hayan sido debidamente autorizados por su superior jerárquico.
- Existe definido un time-out en el fichero, de manera que transcurrido un periodo de inactivad se produce la desconexión de la aplicación de acceso al fichero.
- Los usuarios deben modificar la contraseña de acceso al fichero periódicamente.

f) En la aplicación informática CAUPOL se registran los accesos realizados al fichero PERPOL por parte de los usuarios: persona que lo ha efectuado, datos consultados, día, hora y año de la consulta, así como el ordenador desde el que se ha efectuado el acceso.

2. Los inspectores de la Agencia solicitan a los responsables de la Unidad de Documentación de Españoles y Archivo que les faciliten el acceso al fichero PERPOL y, en particular, a la aplicación CAUPOL de CONTROL DE ACCESOS DE USUARIOS realizando las siguientes comprobaciones:

a) A través del número de ordinal xxxxxxx se accede a los datos relativos a ***D. B.B.B.***, verificándose que las fotografías que figuran en su reseña coinciden con las publicadas en el diario "El Mundo". Se obtiene impresión de pantalla del acceso realizado.

b) A través del mismo número de ordinal se accede a través de CAUPOL a los códigos de los usuarios que accedieron en el mes de marzo a los datos relativos a ***D. B.B.B.***, verificándose que constan los dos accesos mencionados, realizados por un usuario destinado en la plantilla de "(.....)-COMISARÍA LOCAL". Se obtiene impresión de pantalla de la consulta realizada y del resultado de la misma.

3. Con fecha 23 de septiembre de 2009 se envió un escrito de solicitud de colaboración a la DIRECCIÓN ADJUNTA OPERATIVA del CUERPO NACIONAL DE POLICÍA,

solicitando diversa información. En su respuesta realiza las siguientes manifestaciones:

a) En la actualidad las diligencias policiales relacionadas con los hechos aquí descritos y practicadas por la Unidad de Asuntos Internos, son objeto, a su vez, de Diligencias Previas en un Juzgado de Instrucción.

b) En este sentido, en el marco de las citadas diligencias policiales, se recibió declaración, como imputado, a un funcionario del Cuerpo Nacional de Policía, escala básica, destinado en la Comisaría de (.....), como presunto autor de los hechos denunciados.

c) Según informa la Unidad de Asuntos Internos, se tiene conocimiento de que el titular del Juzgado de Instrucción competente procedió a imputar al citado funcionario.

TERCERO: Con fecha 27 de enero de 2010 se acordó iniciar procedimiento de declaración de infracción de las Administraciones Públicas a la ***DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL (CUERPO NACIONAL DE POLICÍA)***, por la presunta infracción de los artículos 9.1 y 10 de la LOPD, tipificada la infracción referida al artículo 9.1 como grave en su artículo 44.3. h) y la referida al artículo 10 como muy grave en su artículo 44.4. g).

CUARTO: Con fecha 1 de marzo de 2010, se remitió por la ***Dirección Adjunta Operativa del Cuerpo Nacional de Policía*** un informe de la ***Subdirección General de Gestión Económica, Técnica y Documental*** (Unidad de Documentación de Españoles y Archivo).

En el mismo se indica que el Grupo VIII de la Unidad de Asuntos Internos del Cuerpo Nacional de Policía, tras la publicación de la ficha policial del denunciante inició una investigación interna para averiguar la persona o personas que accedieron a la información y que pudieron facilitarla a los medios de comunicación. Esta investigación dio como resultado la constatación de un acceso que no estaba suficientemente justificado.

QUINTO: Con fecha 20 de abril de 2010, se acordó por la instructora del procedimiento la apertura de un período de práctica de pruebas, teniéndose por incorporadas las actuaciones previas de investigación, E/01194/2009, así como las alegaciones y demás documentación aportada por la ***DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL (CUERPO NACIONAL DE POLICÍA)***.

SEXTO: Con fecha, 1 de julio de 2010, la instructora del procedimiento emitió Propuesta de Resolución, en el sentido de que por el Director de la Agencia Española de Protección de Datos se declare que la ***DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL (CUERPO NACIONAL DE POLICÍA)*** ha infringido lo dispuesto en el artículo 10 de la LOPD, infracción tipificada como muy grave en el artículo 44.4.g) de dicha norma. Asimismo se requiere al organismo denunciado para que adopte las medidas de orden interno que impidan que en futuro pueda producirse una nueva infracción del artículo 10 de la LOPD.

SÉPTIMO: Transcurrido el plazo de 15 días hábiles concedido a las partes para realizar alegaciones a la propuesta de resolución de este procedimiento, no se han recibido en esta Agencia escrito de alegaciones ni del denunciante ni del organismo denunciado.

HECHOS PROBADOS

PRIMERO: En el mes de febrero de 2009, en el marco de las diligencias previas nº ###/**** llevadas a cabo por el Juzgado de Instrucción nº 0A de ...., se acordó la detención de D. ***B.B.B.*** (en adelante el denunciante) por las Fuerzas y Cuerpos de Seguridad del Estado (folio 1).

SEGUNDO: La ***Dirección General de la Policía y de la Guardia Civil (Cuerpo Nacional de Policía)*** (en lo sucesivo el organismo denunciado), elaboró la correspondiente ficha policial del denunciante donde se recogían datos personales del mismo tales como nombre, apellidos, domicilio, D.N.I., filiación, fecha de nacimiento, huella digital y fotografías (folios 20 y 21).

TERCERO: El 12 de marzo de 2009, salieron publicadas las fotografías de la ficha policial del denunciante en varios medios de comunicación (folios 8, 9 y 10). Las fotografías se corresponden con las de la ficha policial ya que son idénticas y en todas ellas es perfectamente visible el número **** con el que aparecen clasificadas en el fichero PERPOL del organismo denunciado (folio 21).

CUARTO: El 13 de marzo de 2009, la Unidad de Documentación de Españoles y Archivo del organismo denunciado, elabora una nota informativa con el siguiente asunto "fotografías reseña de la base de datos PERPOL de ***B.B.B.***, aparecidas en el Diario "EL MUNDO", del día dd/mm/aaaa" (folio 18). En esta nota informativa se concluye que las fotos pertenecen a la reseña policial recogida en el fichero PERPOL.
A través de la aplicación de control del fichero anteriormente citado, CAUPOL, se ha tenido constancia de siete accesos en ese período de tiempo: tres accesos correspondientes a funcionarios destinados en la unidad del organismo denunciado que tramita las reseñas y fichas policiales; dos accesos de un funcionario destinado en la unidad del organismo denunciado que interviene en la instrucción de la diligencias previas por las que el denunciante está imputado; y dos accesos de un funcionario destinado en una comisaría de (.....) (folios 18 y 19).

QUINTO: El 16 de marzo de 2009, el Grupo VIII de la Unidad de Asuntos Internos del organismo denunciado inicia una investigación interna para esclarecer la forma en que las fotografías de la reseña policial del denunciante salieron del fichero PERPOL. Se tramita el atestado policial xx/++ para poner a disposición judicial al funcionario destinado en la comisaría de (.....) cuyos accesos a los datos del denunciante en el fichero PERPOL no estaban suficientemente motivados (folios 32, 33 y 72).

SEXTO: En la actualidad el Juzgado de Instrucción nº 0B de (.....) instruye las Diligencias Previas **+/## en las que consta como imputado el funcionario del Cuerpo Nacional de Policía de la escala básica, destinado en la comisaría de (.....) como presunto autor de delitos de revelación de secretos, descubrimiento de secretos, violación de secretos y cohecho (folios 32, 33 y 72).

SÉPTIMO: El representante legal del denunciante interpuso el 13 de marzo de 2009, denuncia ante la Agencia Española de Protección de Datos por los hechos anteriormente relatados. Esta denuncia dio origen a los siguientes procedimientos: E/04034/2009 y E/04035/2009 contra varios medios de comunicación y el procedimiento que nos ocupa AP/00081/2009 frente a la Dirección General de la Policía y de la

Guardia Civil (Cuerpo Nacional de Policía). En los dos procedimientos citados primeramente se acuerda no incoar actuaciones inspectoras y no iniciar procedimiento sancionador o de infracción de las Administraciones Públicas.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver este procedimiento el Director de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37.g) en relación con el artículo 36 de la LOPD.

II

Antes de entrar de lleno en el análisis del asunto que aquí nos ocupa, se debe modificar la calificación de una de las posibles infracciones recogidas en el acuerdo de inicio de este procedimiento. En concreto la vinculada a la posible vulneración del artículo 10 de la LOPD y a la que se aludía en el fundamento jurídico segundo del acuerdo de inicio citado. En dicho fundamento se señalaba que la posible vulneración del deber de secreto recogido en el artículo 10 de la LOPD, se tipificaba en esta ley como una infracción grave y así se establecía en el artículo 44. 3 g) de dicha norma legal. El tenor literal de la misma expresa que son infracciones graves:

> "g) la vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo."

No obstante lo anterior, nos encontramos con una posible vulneración del deber de secreto de los datos recogidos en el fichero denominado PERPOL y cuyo responsable es el organismo denunciado. Se trata de un fichero policial y los datos que se han revelado no hacen referencia aún, a una infracción penal pues no ha recaído sentencia judicial firme en el Juzgado que instruye la causa en la que el denunciante aparece como imputado. Así pues, estos datos se han recabado con fines policiales y esta circunstancia exige que se cambie la calificación de la posible infracción, pasando de grave a muy grave tal y como se recoge en el artículo 44.4 g) de la LOPD que dispone que son infracciones muy graves:

> " g) la vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas."

III

Tal y como se ha señalado en el fundamento anterior, la posible vulneración del deber de secreto afecta a datos recogidos en el fichero PERPOL, que es un fichero de las Fuerzas y Cuerpos de Seguridad y al que afecta lo establecido en el artículo 22 de la LOPD:

> "1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.
>
> 2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad..."

Dentro de los ficheros de las Fuerzas y Cuerpos de Seguridad se distingue entre ficheros con fines administrativos y ficheros con fines policiales. Para recabar y tratar datos recogidos en ficheros con fines policiales como el PERPOL, no es necesario el consentimiento del titular de los datos y por ello constituyen una excepción al principio básico en la normativa de protección de datos que exige tener el consentimiento del afectado para el tratamiento de datos de carácter personal. El resto de principios básicos recogidos en la LOPD deben ser respetados por este tipo de ficheros, y entre ellos el deber de secreto regulado en el artículo 10 de la citada norma legal que obliga al responsable del fichero y a cuántos intervengan en el tratamiento de los datos, al secreto profesional sobre los mismos y al deber de guardarlos.

Tal y como se ha indicado en el fundamento primero, la vulneración del deber de secreto en los ficheros con fines policiales dará lugar a la infracción calificada como muy grave del artículo 44.4 g) de la LOPD.

IV

En este supuesto se imputa también al organismo denunciado, la posible infracción del artículo 9.1 de la LOPD que se refiere a la seguridad de los datos en los siguientes términos:

> "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."

Tal y como dispone el artículo 44.3.h) de la LOPD "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" constituirá una infracción grave.

PERPOL es un fichero con fines policiales y como tal, el responsable del mismo deberá implantar medidas de seguridad de nivel alto, tal y como establece el artículo 81.3.b) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD (en lo sucesivo RLOPD):

> "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:
> …b) los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas."

Esta exigencia viene recogida también en la Orden INT/1751/2002, de 20 de junio por la que se regulan los ficheros informáticos de la Dirección General de la Policía que contienen datos de carácter personal, adecuándolos a las previsiones establecidas en la LOPD y demás normativa sobre la materia; en el anexo de esta norma legal se establece un nivel alto para las medidas de seguridad a adoptar en el fichero PERPOL.

V

En el caso que nos ocupa podemos afirmar que las fotografías del denunciante tienen su origen en el fichero PERPOL de la Dirección General de la Policía y de la Guardia Civil. El propio organismo denunciado ha reconocido que la información salió de este fichero. Las fotografías publicadas son coincidentes con las tomadas en la reseña policial que se hizo del denunciante tras su detención como imputado en una causa penal.

La fotografía, al plasmar la imagen de una persona de tal forma que se la pueda identificar, constituye un dato de carácter personal y como tal sometido a las exigencias de la LOPD. El artículo 5.1.f) del RLOPD a la hora de definir lo que se entiende por dato de carácter personal indica que se entenderá por tal:

> "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables."

Nos encontramos por tanto, con datos personales (fotografías) del denunciante que formando parte de un fichero con fines policiales (PERPOL) aparecen publicados en distintos medios de comunicación sin el consentimiento de su titular. El responsable de este fichero que contiene datos de carácter personal debe cumplir con las exigencias de la LOPD. Entre ellas y como ya se ha señalado anteriormente, el deber de secreto de los datos que trata y la obligación de adoptar medidas que garanticen la seguridad e integridad de los datos que forman parte del fichero.

Llegados a este punto debe analizarse si los hechos relatados constituyen una infracción del deber de secreto recogido en el artículo 10 de la LOPD tipificada como muy grave por afectar a ficheros con fines policiales o una infracción de la seguridad de los datos regulada en el artículo 9 de la LOPD y tipificada en esta normal legal como infracción grave.

En lo concerniente a las medidas de seguridad que deben implantarse en el fichero PERPOL, al ser un fichero con fines policiales el nivel exigido es el más alto (nivel alto). Tanto en las alegaciones realizadas por el organismo denunciado como en el acta de la inspección llevada a cabo por inspectores de esta Agencia se concluye que:

> se ha adoptado un control de accesos restringido y limitado al fichero PERPOL, únicamente pueden acceder los funcionarios del organismo denunciado que cuentan con autorización expresa para ello. Para la concesión de esta autorización se requiere que se formalice una petición por el responsable policial del funcionario propuesto justificando la necesidad de la misma para el desarrollo de las funciones que éste tiene encomendadas.
>
> la autorización implica la asignación de un usuario, que coincide normalmente con el número del Documento Nacional de Identidad, más una

clave y una contraseña de libre designación por cada usuario. Estas últimas son obligatoriamente cambiadas de forma periódica al exigirlo la propia aplicación.

existe definido un time-out en el fichero, de manera que transcurrido un período de inactividad se produce la desconexión de la aplicación de acceso al fichero.

se dispone de una aplicación, CAUPOL, que permite la realización de auditorías de los accesos realizados, persona que lo ha efectuado, datos consultados, día, hora y año de la consulta, así como el ordenador desde el que se ha efectuado el acceso.

las solicitudes de autorizaciones se centralizan y se valoran en la Unidad de Documentación de Españoles y Archivo, concediéndose previo el cumplimiento de los requisitos antes expuestos.

El fichero PERPOL reúne las condiciones exigidas por la LOPD y a través de la aplicación CAUPOL, control de accesos de usuarios, el organismo denunciado pudo comprobar que entre los días 11 de febrero a 4 de marzo de 2009, hubo siete accesos a la ficha policial del denunciante pertenecientes a tres usuarios diferentes autorizados conforme al protocolo establecido al efecto y que se acaba de describir.

De lo anteriormente expuesto, se infiere que el organismo denunciado aplica las normas de seguridad que exige la normativa de protección de datos para ficheros con fines policiales y en consecuencia, no se le puede imputar una infracción del artículo 9 de la LOPD.

VI

Se imputa también al organismo denunciado la infracción del artículo 10 de la LOPD que regula el deber de secreto en los siguientes términos:

> "el responsable del fichero y quieres 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 aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."

El citado artículo 10, regula de forma individualizada el deber de secreto de quienes tratan datos personales, dentro del título dedicado a los principios de protección de datos, lo que refleja la gran importancia que el legislador atribuye al mismo.

El deber de secreto trata de salvaguardar o tutelar el derecho de las personas a mantener la privacidad de sus datos de carácter personal y en definitiva el poder de control o disposición sobre sus datos. Este deber de secreto está lógicamente relacionado con el secreto profesional, tiene la misma fundamentación jurídica, pero el deber de secreto de la LOPD se refiere al ámbito estricto del tratamiento de los datos personales, en el que el responsable del fichero y, cualquier persona que intervenga en el tratamiento, está obligado a mantener la confidencialidad de los datos personales y no pueda revelar ni dar a conocer su contenido.

El deber de secreto tal y como viene declarando la Audiencia Nacional, entre otras en su Sentencia de 14 de septiembre de 2001 (recaída en el recurso nº 196/2000):

> "resulta esencial en las sociedades actuales cada vez más 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 Constitución Española."

En sus alegaciones el organismo denunciado pone de manifiesto que en su auditoria interna se concluyó que un funcionario de su plantilla facilitó las fotografías del denunciante a los medios de comunicación. Y se fundamente en este hecho para afirmar que "*la responsabilidad que se deriva del artículo 10 de la LOPD sólo puede ser una responsabilidad personal que obliga a título personal, a aquellos a los que va dirigido sin que su incumplimiento pueda achacarse al órgano gestor del fichero…El deber de secreto profesional afecta a aquel al que va dirigido y sólo él es el responsable de su incumplimiento*."

A pesar de las alegaciones del organismo denunciado, en lo que a la protección de datos atañe no puede tenerse en cuenta la afirmación de que el deber de secreto es un deber que se exige a título personal. El artículo 43.1 de la LOPD determina que:

> "los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente ley."

Así pues en virtud de este artículo sólo los responsables de los ficheros y los encargados de los tratamientos pueden ser sujetos activos del régimen sancionador establecido en la LOPD, pues sólo a ellos les es aplicable el régimen sancionador que se diseña en la ley por medio de su artículo 43.1.

El responsable del fichero PERPOL es el organismo denunciado, la Dirección General de la Policía y de la Guardia Civil, ya que tal y como define el artículo 3 d) de la LOPD, se entiende por responsable del fichero "*a toda persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento*." Como responsable del fichero, el organismo denunciado, por indicación expresa de la ley, está sujeto a su régimen sancionador.

Hay que señalar que la infracción del deber de secreto es una infracción de resultado y así lo ha establecido la Audiencia Nacional entre otras en la sentencia recaída en el recurso 205/2008 donde expresamente se señala:

> "esta Sala tiene establecido como la infracción del deber de secreto es una infracción de resultado en la que lo relevante es que se llegue a producir la divulgación de un secreto",

o en la recaída en el recurso 471/2008 cuyo tenor literal expresa

> "la infracción tipificada en el art. 44.3 g) es una infracción de resultado que exige que los datos personales sobre los que exista un deber de secreto profesional…se hayan puesto de manifiesto a un tercero…"

Así pues lo relevante en esta infracción es que se produzca el resultado, que se vulnere la confidencialidad de los datos cuya custodia corresponde al responsable del fichero. En este caso la confidencialidad se ha vulnerado al poner de manifiesto a terceros los

datos personales del denunciante que posteriormente aparecieron publicados en varios medios de comunicación.

VII

Una vez analizados los hechos, debe hacerse una mención a la actuación del organismo denunciado ante los hechos que aquí se examinan, ya que neutralizó en gran medida el efecto antijurídico de la infracción que se le imputa. Hay que destacar la capacidad de reacción del organismo denunciado a la hora de averiguar quién o quienes facilitaron la información del denunciante a los medios de comunicación. Gracias a la rapidez con que se emprendió dicha investigación se obtuvieron de inmediato resultados concluyentes.
Asimismo la investigación interna se llevó a cabo de oficio y al presunto infractor se le puso de forma inmediata a disposición del Juzgado de Instrucción nº 0B de (.....) que en la actualidad instruye diligencias previas en relación con los hechos aquí expuestos.

No obstante lo anterior durante el procedimiento ha quedado acreditado que se ha producido una vulneración del deber de secreto regulado en el artículo 10 de la LOPD, y que dicha vulneración tuvo lugar en el fichero PERPOL del que es responsable el organismo denunciado. A la hora de realizar el juicio de culpabilidad se deben realizar una serie de precisiones. La exigencia de la culpabilidad procede de lo que señala el artículo 130 de la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante LRJPAC) cuando dice que:

> "sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aún a título de simple inobservancia."

La sentencia de la Audiencia Nacional de 27 de mayo de 2010 (Rec. 621/2009) en relación a la culpabilidad señala:

> "así pues una sanción se podrá imponer sin ninguna duda en los supuestos dolosos y en los culposos bastando en estos últimos con la inobservancia del deber de cuidado…La delicada materia a la que se refiere la Ley de Protección de Datos, se traduce en la necesidad de exigir una especial diligencia a las entidades gestoras de los datos…Esa falta de diligencia configura el elemento culpabilístico de la infracción administrativa… y obviamente no precisa de la concurrencia de dolo."

Hay que señalar que si se exige una especial diligencia a las entidades gestoras de los datos, esta será mayor (de ahí la obligación para el responsable del fichero de implantar medidas de seguridad de nivel alto) cuando el fichero contiene datos especialmente sensibles como los que se almacenan en el fichero PERPOL cuya finalidad es la investigación policial.

Si bien no es su causa directa al mediar actuaciones intermedias, la publicación de las fotos del denunciante sin su consentimiento tiene su origen mediato en la infracción del deber de secreto. Dichas fotografías forman parte del fichero PERPOL que pertenece al organismo denunciado que como responsable del mismo, debe implantar, revisar y actualizar las medidas de seguridad que impidan el acceso libre por funcionarios habilitados a datos cuando este acceso no esté justificado por razón de su trabajo.

En definitiva, ha quedado acreditada una vulneración del deber de secreto, que tal y como declara la Audiencia Nacional es una infracción de resultado, en la que lo determinante es que tenga efectivamente lugar el resultado: la puesta de manifiesto a terceros de datos personales del denunciante contenidos en el fichero PERPOL.
Fichero del que es responsable el organismo denunciado que a pesar de haber reaccionado inmediatamente ante la situación, al no haber observado el deber de cuidado necesario para que no se produjera el resultado aquí expuesto, debe responder por la infracción del artículo 10 de la LOPD.

Por todo lo anterior, se insta al organismo denunciado para que en el futuro adopte las medidas que eviten actuaciones como la que ha derivado en el presente procedimiento de infracción. Las medidas adoptadas deberán ponerse en conocimiento de esta Agencia.

VIII

Por último hay que hacer una mención a la solicitud por parte del representante legal del denunciante de una indemnización por los daños ocasionados en su persona por los hechos denunciados. Se debe indicar que si bien los afectados pueden reclamar una indemnización por los daños sufridos como consecuencia del incumplimiento de la LOPD tal y como expresa el artículo 19 de esta norma legal, dicha indemnización deberá exigirse en su caso, de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas, y someterse a sus reglas propias. Sin perjuicio de que por parte de este organismo no se deduce una vinculación directa e inmediata entre la vulneración del deber de secreto y la divulgación en prensa de las fotografías del denunciante.

Vistos los preceptos citados y demás de general aplicación,

El Director de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: **PROCEDER AL ARCHIVO** del presente procedimiento en relación con la infracción del artículo 9 de la LOPD calificada como grave en el artículo 44.3 h) de la misma norma legal.

SEGUNDO: **DECLARAR** que la ***DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL (CUERPO NACIONAL DE POLICÍA)*** ha infringido lo dispuesto en el artículo 10 de la LOPD, infracción tipificada como muy grave en el artículo 44.4.g) de dicha norma.

TERCERO: **REQUERIR** a la ***DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL (CUERPO NACIONAL DE POLICÍA)*** para que adopte las medidas de orden interno que impidan que en el futuro pueda producirse una nueva infracción del artículo 10 de la LOPD.

Las resoluciones que recaigan en relación con las medidas y actuaciones adoptadas, deberán ser comunicadas a esta Agencia Española de Protección de Datos, de acuerdo con el artículo 46.3 de la LOPD. La citada comunicación deberá realizarse en el plazo de un mes.

CUARTO: **NOTIFICAR** la presente Resolución a la ***DIRECCIÓN GENERAL DE LA POLICÍA Y DE LA GUARDIA CIVIL (CUERPO NACIONAL DE POLICÍA)*** y a ***D. A.A.A.*** en representación de D. ***B.B.B.***.

QUINTO: **COMUNICAR** la Resolución que se adopte al **DEFENSOR DEL PUEBLO** de conformidad con lo establecido en el artículo 46.4 de la Ley Orgánica 15/1999.

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, se podrá 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 lo sucesivo 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.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la 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.

Madrid, 26 de julio de 2010

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: Artemi Rallo Lombarte