



Expediente N°: E/02046/2017

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos, en virtud de denuncia presentada por Doña **D.D.D.**, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 10 de marzo de 2017, tuvo entrada en esta Agencia un escrito remitido por Doña **D.D.D.** y su esposo Don **C.C.C.**, en el que exponen lo siguiente: Don **B.B.B.o** presentó una queja ante la Comisión Disciplinaria del Consejo General del Poder Judicial contra el Sr. **C.C.C.**, Magistrado del Tribunal Superior de Justicia de Extremadura, presentando diversos medios de prueba; entre ellos el documento numerado con el 3. El citado documento no solo se presentó ante la Comisión Disciplinaria, sino también se entregó en la dirección de correo electrónico: **A.A.A.**, que corresponde a la trabajadora del Ayuntamiento de Badajoz, **E.E.E.**, y que no tiene ninguna relación con SegurcaixaAdeslas. En el documento se relatan las vicisitudes laborales de Doña **D.D.D.** con la entidad SegurcaixaAdeslas. A los efectos de esta denuncia se señala que la documentación enviada por SegurcaixaAdeslas contiene datos sensibles que se han trasladado a un tercero, Doña **E.E.E.**, que lo ha podido comunicar a terceros. Añaden que en el documento 3 mencionado, en su página 3, se relatan una serie de manifestaciones falsas y carentes de rigor, que se dice realizó Don **C.C.C.** sin que se le haya pedido consentimiento, informado de acuerdo con lo establecido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD), y vulnerando el deber de secreto al habérselo facilitado a Doña **E.E.E.**

Tras solicitar información complementaria a los denunciados, informan que Doña **E.E.E.** es la esposa del denunciado, desconociendo la fecha en que pudo recibir el mensaje referido a la Sra. **D.D.D.**

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 solicitó información a Don **B.B.B.** acerca de los reenvíos efectuados del correo electrónico referido a la vida laboral de la denunciante, así como sobre la titularidad del correo electrónico **A.A.A.**
2. Don **B.B.B.** ha informado que la remitente del correo es su abogada, Doña **F.F.F.** y la dirección de correo **A.A.A.** es su correo personal y de su familia.

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).

El artículo 126.1, apartado segundo, del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal establece:

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

II

Los denunciantes señalan, en primer lugar, que el denunciado ha vulnerado el deber de secreto ya que se ha enviado información referida a informes laborales de la Sra. **D.D.D.** (con la que trabajaba en Adeslas SegurCaixa) a un correo electrónico de su esposa, trabajadora del Ayuntamiento de Badajoz.

El artículo 10 de la LOPD dispone: *“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.

Este deber de secreto comporta que el responsable de los datos almacenados no pueda 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 o, en su caso, con el responsable del mismo”*. Este deber es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30/11, y por lo que ahora interesa, comporta que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

Este deber de sigilo 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 efecto, este precepto contiene un *“instituto de garantía 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”*



(Sentencia del Tribunal Constitucional 292/2000, de 30/11). Este derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino 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.

La Sentencia de la Audiencia Nacional, Sección 1ª de la Sala Contencioso-administrativa, de fecha 18 de junio de 2009, indica lo siguiente con referencia al deber de secreto:

<<Por lo tanto, resulta que no se ha acreditado que se haya producido ninguna forma de infracción del deber de secreto pues 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.

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, no siendo relevante (a los efectos de la violación del deber de secreto) con la simple omisión de medidas de seguridad.

En la sentencia correspondiente al recurso 471/2008 se expuso expresamente esta cuestión razonando del siguiente modo: <<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 -como aquí ocurre en relación con el número de la cuenta corriente- se hayan puesto de manifiesto a un tercero, sin que pueda presumirse que tal revelación se ha producido. Efectivamente, la Agencia Española de Protección de Datos en su resolución se limita a poner de manifiesto que el sistema de cierre, mediante ventanilla transparente, de los sobres utilizados por el Banco para realizar determinadas comunicaciones a sus clientes pudiera dar lugar a que determinados datos personales contenidos en esas comunicaciones puedan ser conocidas por terceras personas respecto de las que deba mantenerse el secreto. No prueba sin embargo que los datos fueran efectivamente conocidos por dichos terceros. Estaríamos, por tanto, como sostiene el recurrente, ante una posible infracción de medidas de seguridad -que es una infracción de actividad- pero no ante la infracción que se le imputa que exige la puesta en conocimiento de un tercero de los datos personales.

Por otro lado, tampoco se deduce de la observación del sobre que fue aportado junto con la denuncia -ya abierto y rotos sus mecanismos de confidencialidad- que la revelación del número de la cuenta corriente pudiera producirse (al estar roto tal comprobación no es posible) y en el propio Acta de Inspección levantada el 21 de noviembre de 2007 se hace constar que los inspectores solicitaron el acceso a los sobres utilizados por OPEN BANK para remitir documentación a sus clientes por Postal Express, verificando que a través de la ventanilla que contiene no es posible visualizar el número de cuenta bancaria del cliente. Por tanto, además de no haberse acreditado la revelación de datos personales a persona alguna, tampoco se ha acreditado que el sistema de ensobrado utilizado por la parte recurrente para la realización de determinados envíos postales permita que dicha revelación sea posible.>>



Aplicando ese mismo criterio, resulta que en el caso presente no se ha llegado a producir divulgación alguna por lo que no se justifica la imposición de la sanción derivada de una revelación de secretos que no se llegó a producir.>>

Durante las actuaciones previas de investigación, Don **B.B.B.** ha expuesto que el correo objeto de denuncia fue remitido por su abogada al correo que utiliza en el ámbito familiar. No existe constancia de que la esposa del denunciante haya accedido y leído la información laboral de Doña **D.D.D.**, por lo que no se acredita el incumplimiento de la infracción denunciada.

III

Añaden los denunciantes que en el documento de denuncia enviado al Consejo General del Poder Judicial, se relatan una serie de manifestaciones falsas y carentes de rigor, que se dice realizó Don **C.C.C.**, sin que se le haya pedido consentimiento, informado de acuerdo con lo establecido en el artículo 5 de la LOPD.

El artículo 11 de la LOPD señala:

"1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

...d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas".

Junto a lo anterior, hemos de tener en cuenta lo establecido en el artículo 24 de la Constitución Española, que en lo relativo al derecho constitucional a la "Tutela Judicial Efectiva", su punto 2º nos dice: "asimismo, todos tienen derecho a utilizar los medios de prueba pertinentes para su defensa."

Tal y como sostiene reiterada jurisprudencia del Tribunal Constitucional (por todas, STC 186/2000, de 10 de julio, con cita de otras muchas) "el derecho a la intimidad no es absoluto, como no lo es ninguno de los derechos fundamentales, pudiendo ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho".

Por tanto, normativamente se ha establecido la correspondiente previsión, referida a la utilización de medios probatorios por las partes para el procedimiento seguido en cada caso.

A partir de lo anterior, y aun cuando no mediase consentimiento de los titulares para el tratamiento de sus datos, debe partirse de la premisa de que ningún derecho es



absoluto y que puede ceder ante intereses constitucionalmente relevantes. En este caso concreto, el denunciado interpone una denuncia contra el órgano competente para dilucidarla, el Consejo General del Poder Judicial.

Por otra parte, la Sentencia de la Audiencia Nacional de 8 de marzo de 2012, da una interpretación extensiva al artículo 11.2.d) de la LOPD, de forma que no sólo cubre los datos solicitados directamente por los Jueces y Tribunales, sino también aquellos obtenidos por las partes y aportados al proceso como prueba y que han sido admitidos como tal. En concreto, la SAN resuelve lo siguiente:

“Ha de tenerse en cuenta, además, que una de las causas que excluye la necesidad de consentimiento para la cesión de datos personales, es que la comunicación que deba efectuarse tenga por destinatarios a los Jueces o Tribunales (Art. 11.2.d) LOPD). Excepción en la que no es descabellado incluir aquellos supuestos en que se trata de pruebas que, si bien no han sido solicitadas por el Juez o Tribunal, sino aportadas por las partes, con posterioridad no consta que las mismas hayan sido rechazadas, sino incorporada por el Juez a las actuaciones, tal y como, al parecer, ocurrió en el presente supuesto”.

De lo expuesto se infiere que el denunciado trató los datos de Don **C.C.C.** para denunciarlo, teniendo como destinatario al órgano competente para tratar su denuncia; no siendo necesario el consentimiento del denunciado para proceder al tratamiento de sus datos y para su cesión al Consejo General del Poder Judicial.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a Don **B.B.B.**, Doña **D.D.D.**, y Don **B.B.B.**.

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 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.

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