Expediente Nº: E/04271/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la Universidad Complutense de Madrid, en virtud de denuncia presentada por el ******CARGO.1*** de la Facultad de ***XXXXX*** Don ***A.A.A.,*** y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 28 de junio de 2013, tuvo entrada en esta Agencia Española de Protección de Datos un escrito remitido por Don ***A.A.A.*** en el que declara lo siguiente:

> Los días 19 y 20 de junio de 2013, se recibió de forma masiva un correo electrónico dirigido a los profesores y personal de la Facultad de ***XXXXX*** de la Universidad Complutense.
>
> El correo tenía como dirección de origen ***.....@gmail.com,*** y el remitente se identificaba como ***B.B.B.***.
>
> Que dicho nombre no corresponde con ningún alumno del centro.
>
> Que el remitente ha tenido acceso indebido a los correos electrónicos de la citada Facultad, que no son públicos ni de acceso general a terceros.
>
> El correo remitía adjunta una documentación con información reservada relativa a una profesora del Departamento de ***XXXXX***.
>
> Dicha documentación no es original pues carece de sello de registro.
>
> Dicha documentación ha sido alterada respecto de la original, ya que se ha eliminado el nombre de un profesor que en ella aparecía.

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. De las evidencias aportadas con el texto de la denuncia se desprende lo siguiente:

   Se han remitido correos por parte del remitente a las siguientes direcciones:

   - ***.....1@....ucm....***
   - ***.....2@....ucm....***
   - ***.....3@....ucm....***
   - ***.....4@....ucm....***
   - ***.....5@....ucm....***
   - Destinatario no identificado

Las direcciones destinatarias corresponden al dominio ucm.es, que corresponde al de la Universidad Complutense de Madrid. No hay constancia que se hayan enviado correos a direcciones fuera de ese dominio.

Que las direcciones de origen de los correos son ***.....@gmail.com*** y ***.....@outlook.es***.

Que el remitente se identifica no sólo como ***B.B.B.***, sino también como ***C.C.C.***.

Que en el asunto y cuerpo del mensaje se hace referencia explícita a una denuncia de alumnos contra Doña ***D.D.D.,*** profesora de la Universidad en el doble grado de ***XXXXX y XXXXXXXXXXXXXX*** y al Departamento de ***XXXXX*** de la Universidad Complutense de Madrid.

Que los correos tienen un documento anexo titulado "*Denuncia de alumnos contra* ***D.D.D.***"

El documento que se incluye en la denuncia y que se corresponde con el remitido en los correos es un escrito dirigido a la Vicedecana de Calidad e Innovación de la Facultad de XXXXX de la Universidad Complutense en el que se exponen una serie de hechos atribuidos a la Profesora Doña ***D.D.D.***, que se la identifica como Profesora ***Titular de XXXXX de la Universidad Complutense de Madrid y*** Directora de su Departamento ***de XXXXX***.

Dicho documento no hace referencia a terceras personas ni está firmado.

El denunciante aporta otro documento, cuyo origen es la Comisión de Calidad y que tiene sello de registro de entrada en la Facultad de ***XXXXX*** de la Universidad Complutense de Madrid, para que se compare con el texto anterior.

La diferencia entre ambos reside en que el documento que se incluye como remitido adjunto a los correos no tiene el sello de registro de la Universidad y se ha eliminado la referencia al Profesor ***E.E.E.;*** además no aparecen líneas subrayadas.

2. Se remitieron solicitudes de información a Microsoft Ibérica y a Google Inc. solicitando los datos identificativos así como la dirección IP de los titulares de las direcciones de correo ***.....@outlook.es*** y ***.....@gmail.com***, respectivamente.

   De las contestaciones recibidas se constata que el titular del correo Gmail accedió a su cuenta desde las siguientes direcciones IP:

   1. ******IP.1*** entre las 9:00 y las 11:00 horas del día 19 de junio de 2013.
   2. ******IP.2*** entre las 17:00 y las 19:00 horas del día 20 de junio de 2013.
   3. ******IP.3*** entre las 13:00 y las 15:00 horas del día 19 de junio de 2013

3. De la consulta a la base de datos RIPE, como consta en la diligencia de 24 de septiembre de 2013 se estableció que las dos primeras corresponden a redes que están administradas por la Universidad Complutense de Madrid, mientras que la última está administrada por Telefónica de España.

4. Se remitieron solicitudes de información al Centro de Proceso de Datos de la Universidad Complutense de Madrid así como a Telefónica de España para determinar los datos identificativos de los usuarios que tenían dichas direcciones

asignadas en las fechas señaladas.

5. Telefónica de España informó que la dirección IP ******IP.3***, entre las 13:00 y las 15:00 horas del día 19 de junio de 2013, estuvo asignada de forma dinámica al número de teléfono ******TEL.1*** cuyo titular es Don ***E.E.E.***, con NIF ******NIF.1*** con domicilio de instalación en ***(C/.....1)(Madrid)***.

6. Consultado el directorio del Departamento de ***XXXXX*** de la Universidad Complutense de Madrid, como consta en la diligencia de 9 de octubre, aparece como miembro del profesorado Don ***E.E.E.***.

7. El Centro de Proceso de Datos de la Universidad Complutense de Madrid informó que la dirección IP ******IP.2***, se utiliza para dar salida a más de 3000 equipos a Internet.

   A su vez, la dirección IP ******IP.1*** está asignada desde 2005 a Don ***F.F.F.***, que aparece en los listados obtenidos en el punto 8 primero como personal del Aula de Informática de los Servicios Administrativos de la Facultad de ***XXXXX*** de la Universidad Complutense de Madrid, usada por el equipo con dirección MAC **************** desde 2012.

8. Consultada la accesibilidad que desde Internet existe a las direcciones de correo listadas en el punto, como consta en la diligencia de 9 de octubre, se comprueba:

   Que existe una lista de personal de los Servicios Administrativos de la Facultad de ***XXXXX*** de la Universidad Complutense de Madrid, que incluye direcciones de correo electrónico, accesible públicamente desde Internet.

   Que existe una lista de personal del Departamento de ***XXXXX*** Administrativo de la Facultad de ***XXXXX*** de la Universidad Complutense de Madrid, que incluye direcciones de correo electrónico, accesible públicamente desde Internet.

   Que las direcciones siguientes se encuentran en varias entradas al realizar una búsqueda de las mismas en Internet:

   a. ***.....1@....ucm....***
   b. ***.....3@....ucm....***
   c. ***.....5@....ucm....***

   Que, en particular, la dirección ***.....1@....ucm....*** se encuentra en la lista de personal del Departamento de ***XXXXX*** de la Facultad de ***XXXXX*** de la Universidad Complutense de Madrid anteriormente mencionada.

   Que las direcciones siguientes no se encuentran al realizar una búsqueda Internet:

   a. ***.....2@....ucm....***
   b. ***.....4@....ucm....***

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 objeto de la denuncia se circunscribe, expresamente, al acceso indebido a los correos electrónicos de profesores y personal de administración y servicios de la Universidad Complutense que ha podido tener Don ***B.B.B.,*** ya que envió un correo electrónico a distintos destinatarios del colectivo mencionado.

La LOPD traspuso al ordenamiento interno el contenido de la Directiva 95/46, y en su artículo 1 dispone que *"la presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar".*

El artículo 2.1 de la misma Ley Orgánica establece: *"La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los sectores públicos y privados".*

El artículo. 3 de la LOPD establece las definiciones de responsable de fichero o tratamiento, de encargado de tratamiento y de cesión de datos:

"d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

g) Encargado del tratamiento: La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

i) Cesión o comunicación de datos: toda revelación de datos realizada a la persona distinta del interesado."

El artículo 9 de la LOPD dispone lo siguiente:

"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."

El transcrito artículo 9 de la LOPD establece el principio de seguridad de los datos, imponiendo al responsable del fichero la obligación de adoptar las medidas de índole técnica y organizativa que garanticen tal seguridad, así como para impedir el acceso no autorizado a los mismos por ningún tercero.

De acuerdo con la información obtenida durante las Actuaciones Previas de Investigación, se ha constatado que a través de Internet son accesibles tres de las cinco direcciones de correo electrónico que recibieron el correo enviado por Don ***C.C.C.***; otra de las direcciones corresponde a la misma persona cuyos datos si aparecen en internet, y la última de ellas no se encuentra accesible.

No obstante lo anterior, hay que señalar que la persona a la que corresponde la dirección IP desde la que se envió el correo es un profesor del Departamento de ***XXXXX*** de la Universidad Complutense de Madrid, con acceso a las direcciones de correo electrónico del personal docente y administrativo que presta servicios en dicha Universidad, por lo que no se ha producido un acceso indebido a los correos electrónicos de personal al servicio de la Universidad Complutense.

Hay que tener en consideración que la información se ha enviado a un número muy limitado de destinatarios (cinco personas), a los que tiene acceso legítimo el remitente, ya que es un profesor de la Universidad. Asimismo, en la propia denuncia se afirma que la documentación que se adjunta al correo electrónico no es el original, ya que no aparece el sello del Registro, de lo que se desprende que se ha obtenido al margen de los órganos de la Universidad.

En resumen, la persona que ha enviado los correos trabaja en la Universidad; los hechos expuestos versan sobre cuestiones relacionadas con la propia Universidad y su funcionamiento; y se remite a un número reducido de personas que trabajan en la Universidad.

III

En lo que concierne a la remisión del correo electrónico a cinco personas de la Universidad, hemos de indicar que atendiendo al contenido del correo remitido, nos encontramos ante una denuncia acerca del desarrollo de las clases de una profesora de la Universidad, por lo que se configurarían como interesados potenciales en dicha denuncia, tanto la denunciada, como los alumnos del centro, profesores y el personal relacionado con la gestión y administración de la docencia, dado que en dicha denuncia se tratan circunstancias relacionadas con el desarrollo de una determinada asignatura que se imparte en la Universidad. Por tanto, hemos de considerar lo tratado como una información de interés para los destinatarios. En dicho sentido, ha de señalarse lo establecido por la Audiencia Nacional en varias sentencias donde se vienen considerando como legítimas las comunicaciones a interesados de temas que puedan ser de interés para miembros de una asociación o comunidad, como por ejemplo la dictada el 14 de Abril de 2008 (rec 379/2006), cuyo tenor es el siguiente:

"…el denunciante está integrado en la Asociación sancionada en cuanto propietario de una parcela sita en la Urbanización XXXXX y en el seno de esa relación asociativa es legítimo facilitar información a los asociados sobre cuestiones de interés común vinculadas a su actividad

... Indudablemente la presentación de una denuncia contra la Asociación por

parte del afectado, junto con otros, ante la Fiscalía de Sevilla por la realización de unos trabajos de electrificación en la urbanización, era una información cuyo conocimiento era de interés común y vinculada a los fines asociativos."

En un sentido similar, la Sentencia de la Audiencia Nacional de 8 de julio de 2011 indica lo siguiente:

"La Sala considera que la información remitida respecto a la valoración de la productividad, establecida en un sistema de incentivos por objetivos y circunscrita al ámbito de la zona de trabajo, no puede considerarse como vulneración del deber del secreto pues la consecución de los objetivos y el sistema de incentivos que dimana de la productividad entran dentro de la esfera de las relaciones laborales.

En la sentencia del Tribunal Constitucional 142/93, a la que se refiere la parte recurrente si bien con número erróneo, se indica " ***Las retribuciones que el trabajador obtiene de su trabajo no pueden en principio desgajarse de la esfera de las relaciones sociales y profesionales que el trabajador desarrolla fuera de su ámbito personal e íntimo, para introducirse en este último****, y hay que descartar que el conocimiento de la retribución percibida permita reconstruir la vida íntima de los trabajadores." En el presente caso no es exactamente el derecho a la intimidad el que está en juego sino el derecho a la protección de datos, que excede el ámbito estricto de la intimidad personal, pero la sentencia es expresiva respecto a que datos (en el caso de la misma la retribuciones y en este la productividad) están unidos a la esfera de las relaciones laborales de forma que su conocimiento en el ámbito en el que se producen las citadas relaciones y con finalidades que afectan a las mismas no puede considerarse como una vulneración del deber de secreto."*

Asimismo, la Audiencia Nacional, en sentencia de 20 de Abril de 2009, al recurso 561/2007, recogiendo lo anterior, aunque referido al entorno sindical, ha señalado lo siguiente:

"Si bien es cierto que el derecho a la protección de los datos en el caso examinado impide que los datos personales del denunciante --nombre y apellidos-- se incluyan en una página de la Intranet corporativa sin que medie su consentimiento inequívoco, como señala el artículo 6.1 de la Ley Orgánica 15/1999, sin estar amparado por alguna de las excepciones previstas en el apartado 2 del citado precepto. Sin embargo, esta cobertura de la acción sancionadora ha de quebrar cuando la nota informativa difundida por la Sección sindical del centro de trabajo, en este caso Caja Canarias, y en la que constan los datos del denunciante, tiene por finalidad la transmisión de noticias de interés sindical, permitir ese flujo de información entre el Sindicato y sus afiliados, entre los delegados sindicales y los trabajadores, de manera que se permita el ejercicio completo y cabal de la acción sindical, propiciando, como señalaba la doctrina constitucional trascrita en fundamentos anteriores, el desarrollo de la democracia y del pluralismo sindical, mediante este elemento esencial del derecho fundamental a la libertad sindical.

El derecho fundamental a la protección de datos 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. Este <<poder 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 >> (fundamento jurídico séptimo de la STC 292/2000, 30 de noviembre), ha de ceder cuando se enfrenta al ejercicio del derecho a la libertad sindical en los términos en que concurre en este caso, en el que se trata de proporcionar una información propia de la actividad sindical, no entendible sin el dato personal en cuestión, y limitada al ámbito del centro de trabajo.

Carece de sentido, por tanto, informar sobre una querella criminal relativa a unos hechos surgidos con motivo de la actividad sindical, en el seno del propio sindicato, si no puede señalarse la persona contra la que se dirige para que los miembros del sindicato en la empresa puedan estar informados, conozcan y valoren, con todos los elementos de juicio a su disposición, de las contiendas originadas en el ejercicio de la actuación sindical o con motivo de ella, y la proyección sobre los actos posteriores de los afectados, que precisan de ese dato para su pleno entendimiento.

Del mismo modo, conviene señalar que otro de los elementos que confluye en la ponderación de los intereses es el ámbito de la difusión de la información contenida en la nota informativa. La difusión se ha limitado estrictamente el ámbito de la empresa o centro de trabajo que es precisamente la esfera que faculta el artículo 8 del la Ley de Libertad Sindical para tener derecho a la información sobre cuestiones que afecten a los trabajadores derivadas de la actividad sindical. Téngase en cuenta que la nota en cuestión se publica en la página Intranet Corporativa, cuya difusión se limita a los trabajadores de dicha entidad financiera, Caja Canarias.

De modo que el derecho a la libertad sindical, en cuya valoración, por cierto, no entra la Agencia de Protección de Datos, ha de prevalecer sobre el derecho a la protección de los datos personales, cuando, como sucede en el caso examinado, la acción sindical ampara la actuación del sindicato recurrente para divulgar entre los trabajadores de los centros los datos precisos, y únicamente necesarios, para el entendimiento de la noticia, teniendo un conocimiento cierto de la información relevante desde el punto de vista sindical."

Por tanto, en la medida en que nos encontramos ante una comunicación ligada a ámbitos de interés para los alumnos, profesores y personal de gestión y administración, y que no consta que se llevara a cabo más allá del círculo de posibles interesados, no se dan las circunstancias para el inicio de procedimiento sancionador en materia de protección de datos.

En resumen, los hechos denunciados no son sancionables al no apreciarse incumplimiento de la normativa de protección de datos, pero no supone, en modo alguno, que el afectado no encuentre en el ordenamiento jurídico otros medios de garantía y defensa frente a una posible intromisión ilegítima en su esfera jurídica.

Por lo tanto, de acuerdo con lo señalado,

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

SE ACUERDA:

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente Resolución a Don ***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.

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