

**Procedimiento N° PS/00192/2005****RESOLUCIÓN: R/00027/2006**

En el procedimiento sancionador **PS/00192/2005**, instruido por la Agencia Española de Protección de Datos a **D. O.L.F.**, vista la denuncia presentada por **EI SYSTEM COMPUTER, S.A.**, y en base a los siguientes,

ANTECEDENTES

PRIMERO: Con fecha de 17 de enero de 2005, tuvo entrada en esta Agencia un escrito de D. J.M.R., en representación de EI SYSTEM COMPUTER, S.A., (en lo sucesivo EI SYSTEM), en el que denuncia al actualmente ex-trabajador D. O.L.F. por “*poner a pública e indiscriminada disposición*”, a través de internet, documentos confidenciales del departamento de Recursos Humanos de la compañía, algunos de los cuales contenían datos de carácter personal de los empleados.

De la documentación aportada por EI SYSTEM se desprende que entre el 27 de octubre y, al menos, el 23 de noviembre de 2004, a través del foro <http://.....A/.....A/....A/....A>, se publicaron distintos listados con datos de más de 850 trabajadores de la compañía, referidos a nombre y apellidos y puesto de trabajo y, en algunos casos, número de D.N.I. y número de teléfono corporativo.

De dicha documentación se desprende que tales datos fueron remitidos al citado foro por D. O.L.F., desde un ordenador ubicado en el establecimiento de la compañía y al que, a este empleado, se le había permitido el acceso a los datos de los trabajadores por razón del puesto que desempeñaba dentro del Departamento de Compras.

Entre la citada documentación remitida por EI SYSTEM y que, según se desprende del Informe Pericial, elaborado con fecha 12 de noviembre, fue publicada por D. O.L.F. en internet, a través de la página <http://.....A/.....A/....A/....A>, figuran los siguientes listados con datos de carácter personal:

- Listado ordenado alfabéticamente conteniendo el nombre y apellidos y número de D.N.I. de personas, el cual, según consta en Acta de



Inspección E/XXX/XXXX-0/X/XXXX expedida por los Servicios de Inspección de esta Agencia, es un subconjunto del fichero entregado por el Departamento de Recursos Humanos al Departamento de Compras.

- Listado ordenado alfabéticamente conteniendo el nombre y apellidos, destino dentro de la compañía y categoría (“*general*” o “*Cargo 1*”) de personas, el cual, según consta en Acta de Inspección expedida por los Servicios de Inspección de esta Agencia E/XXX/XXXX-0/X/XXXX, permite conocer la habilitación de los trabajadores de la compañía para acceder a sus procedimientos internos (en función de su categoría). Según ha declarado EI SYSTEM, este listado está almacenado en una carpeta de red a la que tienen acceso sólo los “*Cargo 1*”, condición que ostentaba D. O.L.F..
- 4 listados conteniendo nombre y apellidos y número de teléfono móvil corporativo de algunos trabajadores de EI SYSTEM.
- Listado conteniendo nombre y apellidos, número de teléfono corporativo y dirección electrónica corporativa de algunos contactos de la matriz británica de la compañía DIXONS GROUP PLC. Según consta en Acta de Inspección E/XXX/XXXX-0/X/XXXX, tanto éste como los 4 listados antes citados en el párrafo anterior son de conocimiento público por todo el personal de la compañía.

SEGUNDO: Con fecha 5 de septiembre de 2005, el Director de la Agencia Española de Protección de Datos acordó iniciar Procedimiento Sancionador a D. O.L.F. por una posible infracción del artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos de Carácter Personal (en lo sucesivo LOPD) tipificada como leve en el artículo 44.2. e) de dicha norma, pudiendo ser sancionado con multa de 601,01€ a 60.101,21€ de acuerdo con el artículo 45.1 de la citada Ley Orgánica.

TERCERO: Notificado el acuerdo de inicio, el imputado solicitó la aportación de copia del expediente, presentando posteriormente alegaciones en las que, en síntesis, realizaba una serie de manifestaciones negando ser el responsable de la infracción imputada, argumentando que las direcciones IP desde donde se enviaron los mensajes publicados en el foro, si bien pertenecían a su ordenador personal, las mismas son manipulables, y por ello, dicha circunstancia no constituye prueba de cargo suficiente para determinar la comisión de la infracción.



Asimismo, aporta como prueba diversos documentos, entre los que se aprecia un Recurso de Suplicación frente a la Sentencia nº YYY/YYYY, de 5 de abril, del Juzgado de lo Social nº 0A de (...) en el que se recoge el argumentario utilizado en el citado recurso con objeto de demostrar la posibilidad de la modificación de un número de IP asignado a un determinado ordenador, circunstancia que determinaría la insuficiencia de la principal prueba de cargo en virtud de la cual se han denunciado los hechos.

También se aportan, en dichas alegaciones, documentación acreditativa de la descripción del puesto de trabajo de D. O.L.F., en el que se intenta demostrar que éste no tenía acceso a los ficheros publicados, ya que, según sus manifestaciones, *“era “Cargo 1” de evaluación de los productos y no tenía acceso a los archivos que fueron colgados en internet....”*.

CUARTO: Se acordó el inicio del período de práctica de pruebas, dando por reproducidas las actuaciones obrantes en el expediente E/XXX/XXXX-0/X/XXXX.

QUINTO: Con fecha 17 de noviembre de 2005 se inició el trámite de audiencia de conformidad con lo previsto en el artículo 18.4 del Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, que se encuentra vigente de conformidad con lo que dispone la disposición transitoria tercera de la LOPD, poniendo de manifiesto el expediente al presunto responsable concediéndole un plazo de quince días hábiles para formular alegaciones y aportar cuantos documentos estime de interés.

Dichas alegaciones, que tuvieron entrada en esta Agencia posteriormente a ser realizada la propuesta de resolución, reiteran la inocencia de D. O.L.F., al manifestar la inexistencia de pruebas suficientes que acrediten la comisión de la infracción.

SEXTO: Con fecha 14 de diciembre de 2005, por parte del instructor del procedimiento se formuló propuesta de resolución en el sentido de que, por el Director de la Agencia Española de Protección de Datos, se sancione a D. O.L.F. con multa de 601,01€ por la infracción del artículo 10 de la LOPD, tipificada como leve en el artículo 44.2.e) de dicha norma, siendo notificada a los efectos previstos en el citado artículo 1332/1994, concediendo a éste un plazo de quince días para formular alegaciones a la misma.

D. O.L.F. presentó nuevas alegaciones manifestando que no existen pruebas suficientes para imputar la infracción, reiterando, en síntesis, las manifestaciones ya realizadas durante la tramitación del procedimiento, y en especial, que la dirección IP de un ordenador es un dato fácilmente manipulable y, por tanto, no constituye prueba de cargo suficiente que acredite la infracción denunciada.



Con fecha 2 de febrero de 2006 tienen entrada nuevas alegaciones en las que D. O.L.F. aporta una Sentencia de la Sala de lo Social, Sección 0B, del Tribunal Superior de Justicia de (....) de fecha DDMMAA, estimatoria del recurso de suplicación que interpuso frente a la Sentencia nº YYY/YYYY, dictada por el Juzgado de lo Social nº 0A de (....) de 5 de abril de 2005.

HECHOS PROBADOS

PRIMERO: Entre el 27 de octubre y, al menos, el 23 de noviembre de 2004, a través del foro <http://.....A/.....A/...A/...A>, se publicaron distintos listados con datos de más de ... trabajadores de la compañía, referidos a nombre y apellidos y puesto de trabajo y, en algunos casos, número de D.N.I. y número de teléfono corporativo (folios 48 y 335).

SEGUNDO: D. O.L.F. era trabajador de EI SYSTEM en el momento de producirse los hechos denunciados (folio 1)

TERCERO: EI SYSTEM COMPUTER ha aportado copia de la Sentencia nº YYY/YYYY, de 5 de abril, del Juzgado de lo Social nº 0A de (...), por la que se declara procedente el despido de D. O.L.F., considerando probado que *“Al igual que los demás trabajadores que prestan servicios para la demandada, el demandante suscribió en fecha que no consta el denominado ‘Compromiso de Integridad Profesional’, en el que entre otros aspectos, manifiesta conocer las normas y condiciones que figuran en el manual de la empresa ‘Así trabajamos’”* y que en este documento *“se dispone que en caso de tener acceso a información considerada confidencial, es responsabilidad del trabajador ‘mantener la custodia de dicha información y evitar su difusión, tanto de forma intencionada como accidental’* (folio 320).

CUARTO: Como Hecho Probado Décimo de la referida Sentencia figura lo siguiente:

“Para la realización de su trabajo, el demandante ha tenido asignado en la empresa, de forma exclusiva, un equipo informático con la dirección IP nº ###1.

La dirección IP #####1 de la empresa demandada corresponde al ordenador asignado a O.L.F. y éste, al empleado O.L.F..

*Desde la citada dirección I.P. #####1, el día 26-10-2004, por el usuario con seudónimo ‘*****’ se insertaron diferentes archivos de la empresa, en la web <http://.....A/.....A/...A/...A>, relativos a:*

1.- Documentos de RR.HH: con listados de empleados de la demandada, incluyendo sus D.N.I., dirección de correo electrónico, política de personal de tiendas y formulario de solicitud de personal para tiendas



(..)

6.- *Relación de personal de la demandada.*

(...)

9.- *Relación de números de teléfono móvil del personal de la empresa.*

(...)”. (folio 323).

QUINTO: Figura asimismo, como Hecho Probado Décimo de la Sentencia referidos a los archivos difundidos que: *“los citados archivos se hallan ubicados en la carpeta de la demandada denominada ‘procedimientos’, del servidor de documentos, a cuyo acceso está autorizado, entre otros, el demandante”* (folio 324).

SEXTO: Ha sido aportado al procedimiento copia de la Sentencia de la Sala de lo Social- Sección 0B del Tribunal Superior de Justicia de (.....), de fecha DDMMAA en la que se estima el recurso de suplicación interpuesto por D. O.L.F., contra la citada Sentencia YYY/YYYYY apreciándose en su fundamentación jurídica lo siguiente:

- *“...tal y como se desprende de los citados documentos, y tal y como es sabido por cualquier usuario de internet, las últimas cifras de las direcciones IP se asignan por el usuario pueden ser modificadas en cualquier momento, sustituyendo la de un equipo por la de otro o variando cualquiera de ellas, por lo que se admite el motivo refundiéndose los hechos décimo y duodécimo en la siguiente forma, manteniéndose el hecho noveno que no se desvirtúa”.*
- *“Desde la dirección IP #####1, el día 26-10-2004, por el usuario con seudónimo ‘*****’ se insertaron diferentes archivos de la empresa, en la web ‘http://.....A/...A/...A/...A’ relativos a:*

1.- Documentos de RRHH, con listados de empleados, de la demandada, incluyendo sus DNI, dirección de correo electrónico, ..



12.- *Los citados archivos se hallan ubicados en la carpeta de la demandada denominada ‘procedimientos’ del servidor de documentos, a cuyo acceso está autorizado, entre otros, el demandante, existiendo plena coincidencia entre la información contenida en la carpeta de la empresa y la insertada en la página web a que se ha hecho referencia por el usuario ‘*****’. Las direcciones IP son asignadas por la empresa y pueden ser modificadas”.*

- *“Del relato de probados de la sentencia impugnada, resulta (hecho octavo) que el actor, utilizando el nick ‘.....’ accedió a la página P P P P P con el mensaje que se transcribe que en sí mismo no entraña gravedad alguna para determinar una medida sancionadora por parte de la demandada, por cuanto se limita a efectuar sus percepciones desde su situación en la empresa, en uso de su libertad de expresión, garantizada por el artículo 20.1.a) de la Constitución, sin que, por el contrario, conste acreditado que el usuario ‘.....’ fuera el actor, por cuanto, tal y como pone de manifiesto, las últimas cifras de la dirección IP son fácilmente modificables por cualquier usuario desde cualquiera de los ordenadores que estén conectados a la misma línea de internet, pudiéndose utilizar durante el tiempo que se quiera y volver a variarlos, de manera que no queda identificado el actor porque la persona que utilizó tal nick lo hiciera desde la dirección IP que tenía asignada en la empresa,, por lo que es equivocada la afirmación de la juzgadora a quo, sobre la cual se fundamenta la procedencia del despido de que ‘desde su ordenador –de uso exclusivo-, se insertaron en la página web citada, dichos archivos en horas y días en los que el actor se encontraba en su puesto de trabajo”.*

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

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”.

Por su parte el artículo 11 de la citada Ley Orgánica determina:

“Artículo 11. Comunicación de datos

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:

a) Cuando la cesión está autorizada en una Ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

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.

e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores”.



Debe compararse el texto de los artículos 10 y 11 de la LOPD, que definen, respectivamente, los deberes de secreto profesional respecto de los datos de carácter personal que integran el fichero y la prohibición de comunicación, salvo los supuestos previstos, de dichos datos, pues la trasgresión de cualquiera de dichas garantías por parte de quien se responsabiliza del fichero supone, desde un punto de vista meramente fáctico, una conducta semejante, la comunicación de la información que se contiene en el fichero. Así, la distinción entre ambos tipos de garantías exige que la cesión suponga un comportamiento cualificado de la comunicación de datos, cualificación que no puede ser otra que la voluntad de que los datos sirvan para ser tratados de forma automatizada por parte del cesionario, circunstancia que no concurre en este caso, por lo que la comunicación acontecida debe encuadrarse dentro del marco del secreto profesional.

III

El deber de secreto profesional que incumbe a los responsables de los ficheros, recogido en el artículo 10 de la LOPD, 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, y por lo que ahora interesa, comporta que los datos tratados automatizadamente 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). 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.



IV

En el presente expediente y pese a que en la Sentencia nºYYY/YYYY del Juzgado de lo Social nº 0A de (...), contempla como Hecho Probado Décimo la circunstancia de que, desde la dirección IP del ordenador personal del imputado, se realizó el envío de los ficheros publicados conteniendo datos personales de diversos trabajadores de EI SYSTEM al foro anteriormente citado, es necesario apreciar que, en el caso que nos ocupa, la Sentencia, recaída en el recurso de suplicación interpuesto, de la Sala de lo Social nº 0B del Tribunal Superior de Justicia de (.....), se declara “*equivocada la afirmación de la Juzgadora a quo*” y expone en su parte dispositiva que no puede estimarse probado que fuera D. O.L.F. el autor de la publicación en la web de los datos personales de distintos trabajadores de EI SYSTEM, por lo que al estimar ésta última Sentencia “*que no queda identificado el actor*” que publicó los referidos datos personales, no puede ser imputada la comisión de la infracción en el presente procedimiento sancionador, estimándose, por tanto, adecuado el archivo del mismo.

Vistos los preceptos citados y demás de general aplicación,

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

PRIMERO: ARCHIVAR el presente procedimiento sancionador **PS/000192/2005**.

SEGUNDO: NOTIFICAR la presente resolución a **D. O.L.F.**, (C/.....) y a **EI SYSTEM COMPUTER, S.A.**, (C/.....).

CUARTO: 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.

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

AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS



10/10

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.

Madrid, 8 de febrero de 2006

EL DIRECTOR DE LA AGENCIA ESPAÑOLA
DE PROTECCIÓN DE DATOS

Fdo.: José Luis Piñar Mañas