Procedimiento Nº: A/00257/2012

RESOLUCIÓN: R/00423/2013

En el procedimiento A/00257/2012, instruido por la Agencia Española de Protección de Datos a la entidad SINDICATO DE TRABAJADORES DE LA ENSEÑANZA DE EUSKADI STEE/EILAS, vista las denuncias presentadas y en virtud de los siguientes,

ANTECEDENTES

PRIMERO: Con fechas 6 y 23 de marzo de 2012 tienen entrada en esta Agencia sendos escritos de los denunciantes que se relacionan en los anexos, en los que se declara que sus datos personales se han publicado en internet en la dirección web "*www.stee-eilas.....*" a la que han accedido desde el buscador Google, y que esta publicación se ha hecho sin contar con su consentimiento.

En fechas 20 de marzo y 12 de abril de 2012 por la Inspección se constató que los datos personales de diversos trabajadores de la Universidad del País Vasco resultaban públicamente accesibles en el servidor que aloja el sitio web del Sindicato STEE-EILAS, en un fichero denominado "*XXXXX*" ubicado en la carpeta denominada "*XXXXXXXXXX*" fichero que, en tales fechas, permanecía indexado por el buscador Google.

SEGUNDO: Con fecha 26 de noviembre de 2012, el Director de la Agencia Española de Protección de Datos acordó someter a trámite de audiencia previa el presente procedimiento de apercibimiento A/00257/2012. Dicho acuerdo fue notificado a los denunciantes y al denunciado.

TERCERO: Con fecha 14 de diciembre de 2012 se recibe en esta Agencia escrito del denunciado en el que comunica:

"*Que efectivamente, en el contexto de una migración de datos, se albergó por error un fichero informático conteniendo datos de la RPT de la UPV/EHU en un directorio del servidor que aloja la página web del sindicato. (...)*

Dicho fichero no fue enlazado, en ningún momento, en ninguna de las páginas del portal web del sindicato, y buena prueba de ello es que los denunciantes sólo mencionan la posibilidad de acceso al mismo a través del popular buscador Google.

Que si bien reconocemos un error de seguridad (fichero alojado en directorio accesible mediante protocolos internet no seguros), la visibilidad del fichero en la red se hace posible -en este caso- con la intromisión del motor de búsqueda de Google. (...)

Que estimamos que si bien los datos de la RPT expuestos no deben ser de pública difusión en ningún caso, se trata de datos de nivel básico, que los ciudadanos pueden obtener del cruce de las RPT publicadas en boletines oficiales (fuentes de acceso público) y los directorios profesionales que también ampara el REAL DECRETO 1720/2007, de 21 de diciembre, en su artículo 7 como fuente de acceso público."

HECHOS PROBADOS

PRIMERO: En fechas 20 de marzo y 12 de abril de 2012 por la Inspección se constató que los datos personales de diversos trabajadores de la Universidad del País Vasco resultaban públicamente accesibles en el servidor que aloja el sitio web del Sindicato STEE-EILAS, en un fichero denominado "*XXXXX*" ubicado en la carpeta denominada "*XXXXXXXXXXXXXX*" fichero que, en tales fechas, permanecía indexado por el buscador Google.

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

Los hechos denunciados fueron calificados en el Acuerdo de Trámite de Audiencia de este expediente de Apercibimiento como constitutivos de infracción del artículo 10 de la LOPD, tipificada en el artículo 44.3.d) de la citada Ley Orgánica. No obstante, en esta fase del procedimiento, se considera conveniente modificar la calificación jurídica efectuada e imputar al sindicato de Trabajadores de la Enseñanza de Euskadi Stee/Eilas una infracción del artículo 9 de la Ley Orgánica 15/1999, tipificada en el artículo 44.3.h) de la LOPD.

El primero de los derechos que el artículo 135 de la LRJPAC reconoce a favor del presunto infractor es el de que le sean notificados los términos de la acusación, que comprende la información "*de los hechos que se le imputen, de las infracciones que tales hechos puedan constituir y de las sanciones que, en su caso, se les pudiera*

imponer…".

El Tribunal Constitucional ha venido señalando que "*el contenido esencial del derecho constitucional a ser informado de la acusación se refiere a los hechos considerados punibles que se imputan al acusado"* (STC 95/1995). Por el contrario, y a diferencia de lo que acontece con los hechos, el TC, en Sentencia 145/1993 advierte que la comunicación al presunto infractor de la calificación jurídica y de la eventual sanción a imponer no integra el contenido esencial del derecho a ser informado de la acusación. Hasta tal punto es importante la puesta en conocimiento de los hechos constitutivos de la infracción administrativa, que el T.C. ha declarado que las exigencias del artículo 24.2 de la CE se satisfacen fundamentalmente con la sola comunicación de los hechos imputados para poder defenderse sobre los mismos (STC 2/1987 y 190/1987).

III

El artículo 7 del Convenio Nº 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, establece:

"*Seguridad de los datos:*

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados."

El artículo 17.1 de la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, establece:

"Seguridad del tratamiento:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse"

IV

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."

V

Se imputa a la entidad Sindicato de Trabajadores de la Enseñanza de Euskadi Stee/Eilas el incumplimiento del principio de seguridad de los datos personales que constan en sus ficheros. A este respecto, el artículo 9 de la LOPD, dispone:

"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 citado artículo 9 de la LOPD establece el *"principio de seguridad de los datos"* imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen dicha seguridad, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el *"acceso no autorizado"* por parte de terceros.

Para poder delimitar cuáles son los accesos que la LOPD pretende evitar exigiendo las pertinentes medidas de seguridad, es preciso acudir a las definiciones de *"fichero"* y *"tratamiento"* contenidas en la LOPD. En lo que respecta a los ficheros el artículo 3.a) los define como *"todo conjunto organizado de datos de carácter personal"*

con independencia de la modalidad de acceso al mismo. Por su parte, la letra c) del mismo artículo 3 permite considerar tratamiento de datos cualquier operación o procedimiento técnico que permita, en lo que se refiere al objeto del presente expediente, la *"conservación"* o *"consulta"* de los datos personales, tanto si las operaciones o procedimientos de acceso a los datos son automatizados como si no lo son.

Para completar el sistema de protección en lo que a la seguridad afecta, el artículo 44.3.h) de la LOPD tipifica como infracción grave el mantener los ficheros *"...que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen"*.

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la conservación o consulta- de datos personales, es un tratamiento sometido a las exigencias de la LOPD.

b) Los ficheros que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca, están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se refiere a normas reglamentarias, que eviten accesos no autorizados.

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave.

Es necesario analizar las previsiones que el R. D. 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, prevé para garantizar que no se produzcan accesos no autorizados a los ficheros.

El citado Reglamento define en su artículo 5.2 ñ) el *"Soporte"* como el "*objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos*".

Por su parte, en el artículo 81.1 del mismo Reglamento se establece que "*Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico*".

Las medidas de seguridad de nivel básico están reguladas en los artículos 89 a 94, las de nivel medio se regulan en los artículos 95 a 100 y las medidas de seguridad de nivel alto se regulan en los artículos 101 a 104.

Las medidas de seguridad se clasifican en atención a la naturaleza de la información tratada, esto es, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la misma.

El Reglamento citado, distingue entre medidas de seguridad aplicables a ficheros y tratamientos automatizados (Capítulo III Sección 2ª del Título VIII) y las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados (Capítulo IV Sección 2ª del Título VIII).

El citado Reglamento regula:

"Artículo 91. Control de acceso.

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 93. Identificación y autenticación.

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.

2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible."

Así, Sindicato de Trabajadores de la Enseñanza de Euskadi Stee/Eilas está obligado a adoptar, de manera efectiva, las medidas técnicas y organizativas necesarias previstas para los ficheros de la naturaleza indicada, y, entre ellas, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros.

En el caso presente se ha constatado, por la Inspección de esta Agencia Española de Protección de Datos, que en el servidor que aloja el sitio web del sindicato de Trabajadores de la Enseñanza de Euskadi Stee/Eilas resulta accesible, por medio del buscador Google, un listado de los trabajadores de la Universidad del País Vasco con los datos, entre otros, de: nombres, apellidos, DNI, puesto de trabajo y retribuciones. Estos datos eran accesibles fuera del ámbito de los denunciantes sin su consentimiento lo que establece la base de facto para fundamentar la imputación de la infracción del artículo 9 de la LOPD.

La entidad denunciada reconoce un "*error de seguridad (fichero alojado en directorio accesible mediante protocolos internet no seguros)*" que se albergó el fichero informático conteniendo datos de la RPT de la UPV/EHU en un directorio del servidor que aloja la página web del sindicato. Que este fichero no se enlazó en ninguna página del portal web del sindicato y que la visibilidad del fichero en la red es posible por la intromisión del motor de búsqueda Google.

A este respecto cabe contestar que cuando las herramientas de rastreo del motor de búsqueda Google rastrean un servidor web lo analizan desde su raíz y recopilan todos los documentos que se almacenan en las distintas carpetas en que está organizado, siempre y cuando no se hayan previsto restricciones de acceso para esos documentos o carpetas, en cuyo caso estos no serían visibles para las herramientas de rastreo del motor de búsqueda.

A diferencia de las herramientas de rastreo, un usuario convencional accede a un sitio web utilizando un navegador, que le permite navegar por las distintas páginas web enlazadas desde la página de inicio. Es posible, por tanto, que en el servidor web figuren documentos que no han sido enlazados en el sitio web y no resulten directamente accesibles para un usuario convencional. Pero eso no quiere decir que los documentos no resulten públicamente accesibles, sino que no lo son desde las páginas web que configuran el sitio web.

Se expone también que, aunque los datos expuestos no deben ser de pública difusión en ningún caso, son datos de nivel básico y pueden obtenerse por las RPT publicadas en boletines y los directorios profesionales de los previstos en el artículo 7 del Reglamento de la LOPD como fuentes de acceso público.

Con relación a esta cuestión cabe exponer que la publicidad de las Relaciones de Puestos de Trabajo ha sido objeto de varios Informes Jurídicos de esta Agencia Española de Protección de Datos. En concreto en el nº 0167/2006 se expone lo siguiente:

"Por su parte, el artículo 15.3 de la Ley 30/1984, de 2 de agosto, de Medidas para la Reforma de la Función Pública, establece el carácter público de las Relaciones de Puestos de Trabajo, si bien mismo artículo, en sus apartados 1 a) y 1 b) delimita el contenido de las relaciones de puestos de trabajo, indicando que "las relaciones comprenderán, conjunta o separadamente, los puestos de trabajo del personal funcionario de cada Centro gestor, el número y las características de los que puedan ser ocupados por personal eventual así como los de aquellos otros que puedan desempeñarse por personal laboral" y "las relaciones de puestos de trabajo indicarán, en todo caso, la denominación, tipo y sistema de provisión de los mismos; los requisitos exigidos para su desempeño; el nivel de complemento de destino y, en su caso, el complemento específico que corresponda a los mismos, cuando hayan de ser desempeñados por personal funcionario, o la categoría profesional y régimen jurídico aplicable cuando sean desempeñados por personal laboral".

Es decir, la Ley 30/1984 establece, por una parte, que las relaciones de puestos de trabajo serán públicas, pero por otra aclara que su contenido se refiere a la naturaleza del puesto de trabajo y no a los datos referentes a las personas que lo desempeñan en cada momento concreto."

En definitiva, el Sindicato de Trabajadores de la Enseñanza de Euskadi Stee/Eilas, no actuó con la diligencia debida al no adoptar las medidas de seguridad necesarias y suficientes para garantizar la seguridad de los datos de carácter personal, por ello, debe considerarse que ha vulnerado la LOPD

De acuerdo con los fundamentos anteriores, se deduce que por parte del Sindicato de Trabajadores de la Enseñanza de Euskadi Stee/Eilas se ha producido una vulneración del principio de seguridad de los datos, que ha tenido como consecuencia

que el listado de los trabajadores de la Universidad del País Vasco con datos, entre otros, de: nombres, apellidos, DNI, puesto de trabajo y retribuciones, fuera accesible a terceros no autorizados, en el servidor que aloja el sitio web del Sindicato STEE-EILAS, infracción que procede calificar como grave.

La Audiencia Nacional, en varias sentencias, entre otras las de fechas 14 de febrero y 20 de septiembre de 2002 y 13 de abril de 2005, exige a las entidades que operan en el mercado de datos una especial diligencia a la hora de llevar a cabo el uso o tratamiento de tales datos o su cesión a terceros, visto que se trata de la protección de un derecho fundamental de las personas a las que se refieren los datos, por lo que los depositarios de éstos deben ser especialmente diligentes y cuidadosos a la hora de realizar operaciones con los mismos y deben optar siempre por la interpretación más favorable a la protección de los bienes jurídicos protegidos por la norma.

VI

El artículo 44.3.h) de la LOPD, considera infracción grave:

"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".

Dado que ha existido vulneración del *"principio de seguridad de los datos"*, recogido en el artículo 9 de la LOPD, se considera que Sindicato de Trabajadores de la Enseñanza de Euskadi Stee/Eilas ha incurrido en la infracción grave descrita.

VII

La disposición final quincuagésima sexta de la Ley 2/2011 de 4 de marzo de Economía Sostenible (BOE 5-3-2011) ha añadido un nuevo apartado 6 al artículo 45 de la Ley 15/1999 de Protección de Datos en lugar del existente hasta su promulgación del siguiente tenor:

"*Excepcionalmente el órgano sancionador podrá, previa audiencia de los interesados y atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, no acordar la apertura del procedimiento sancionador, y en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada caso resultasen pertinentes, siempre que concurran los siguientes presupuestos:*

a) que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta Ley.

b) Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento".

La Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común –que, al decir de su Exposición de Motivos (punto 14) recoge "*los principios básicos a que debe someterse el ejercicio de la potestad sancionadora de la Administración y los correspondientes derechos que de tales principios se derivan para los ciudadanos extraídos del Texto Constitucional y de la ya consolidada jurisprudencia sobre la materia*"- consagra el principio de aplicación retroactiva de la norma más favorable estableciendo en el artículo 128.2 que "*las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor*".

En el presente supuesto se cumplen los requisitos recogidos en los apartados a) y b) del citado apartado 6. Junto a ello se constata una cualificada disminución de la culpabilidad del imputado teniendo en cuenta que no consta vinculación relevante de la actividad del denunciado con la realización de tratamientos de datos de carácter personal, su volumen de negocio o actividad y no constan beneficios obtenidos como consecuencia de la comisión de la infracción.

Se expone también en las alegaciones al trámite de audiencia previo al apercibimiento que *"Queremos así mismo subrayar que el mero aviso, por parte de los denunciantes, de la circunstancia motivadora de la demanda, hubiera hecho posible reparar, de manera inmediata, el perjuicio causado. Debe tenerse que en cuenta que los denunciantes son compañeros de trabajo, a los que en modo alguno este sindicato desea perjudicar."* A este respecto cabe señalar que, tras las alegaciones al acuerdo del trámite de audiencia, utilizando el buscador Google, se ha intentado localizar la lista cuestionada en este procedimiento con los datos personales de los denunciantes sin que haya sido posible, quedando acreditado que la publicación ha sido retirada. Teniendo en cuenta estas circunstancias, no procede requerimiento alguno.

De acuerdo con lo señalado,

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

SE ACUERDA:

1.- APERCIBIR (**A/00257/2012**) al SINDICATO DE TRABAJADORES DE LA ENSEÑANZA DE EUSKADI STEE/EILAS con arreglo a lo dispuesto en el artículo 45.6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, con relación a la denuncia por infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de la citada Ley Orgánica.

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 esta acto, según lo previsto en el artículo 46.1 del referido texto legal.

2.- NO REQUERIR a la entidad SINDICATO DE TRABAJADORES DE LA ENSEÑANZA DE EUSKADI STEE/EILAS la adopción de las medidas correctoras pertinentes a la infracción denunciada, toda vez que ha quedado acreditado que ya no resulta accesible la lista denunciada con datos personales de los denunciantes.

3.- NOTIFICAR el presente Acuerdo al SINDICATO DE TRABAJADORES DE LA ENSEÑANZA DE EUSKADI STEE/EILAS.

4.- NOTIFICAR el presente Acuerdo a cada uno de los denunciantes y exclusivamente el anexo que les corresponda en el que se incluye su identificación.

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.

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