

Expediente Nº: E/05986/2013

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos en virtud de denuncia presentada ante la misma por D. **B.B.B.** y en base a los siguientes

HECHOS

PRIMERO: Con fecha de 5 de septiembre de 2013 tiene entrada en esta Agencia un escrito de **B.B.B.** en el que declara:

<<Esta vez si que está el correo infectado no hay más que leer el código que he guardado porque el correo lo borre.

No dejo entrar en el ordenador este tipo de correos, no sé qué pretenden por lo visto infectarme esto es acoso.

*Esta IP es la responsable: **F.F.F.** porta un enlace que seguramente tmb está infectado: <http://www.adobe.....> la ip procede de (united kingdom) no me han respondido su abuse, (....@....) ¿por qué me envían correos infectados??>>*

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 la documentación aportada por el denunciante se desprende que:
 - a. El denunciante recibió un mensaje enviado a las cuentas **A.A.A.** y **.....@ A.A.A.** en fecha 4/9/2013 (17:46 h) aparentemente desde la cuenta **.....@ A.A.A.** con asunto "***SPAM*** Scanned Image from a Xerox WorkCentre".

Es decir, aparentemente, el dominio de las cuentas de origen y destino del correo coinciden **A.A.A.**, apareciendo además como aparente origen del mensaje el servidor de correo electrónico **smtp. A.A.A..**

Además, el mensaje contenía un fichero anexo, afirmando el denunciante que estaba infectado.

- b. Se ha podido comprobar que el servidor de correo electrónico **smtp. A.A.A.** tiene la dirección IP **G.G.G.** y está localizada en España.
 - c. Según las cabeceras de Internet aportadas, el mensaje habría

transitado dentro de la red interna en la que está ubicado el servidor de correo, sin embargo el primer salto hacia Internet lo hizo a través de la dirección IP **F.F.F.**, dirección que está radicada en Reino Unido.

Además, el propio sistema de detección de spam del servidor de correo ha detectado errores en la cabecera de correo electrónico, pues aparece la una cabecera opcional en la que consta:

<<"X-Amavis-Alert: BAD HEADER SECTION, MIME error: error: unexpected end of header; ; error: part did not end with expected boundary; ; error: unexpected end of parts before epilogue">>

E igualmente el sistema SPF detecta la falsificación del remitente ("Sender is not authorized") y es por ello que se ha añadido al asunto del mensaje el texto "****SPAM****".

- d. Dadas las incongruencias detectadas en las cabeceras, se concluye que han sido manipuladas, y posiblemente este mensaje haya sido remitido desde un ordenador en Reino Unido cuyo control ha sido tomado por piratas informáticos, no siendo su propietario consciente de ello.
 - e. De las consultas realizadas al DNS se encuentra que la dirección IP origen del mensaje está radicada en Reino Unido y pertenece a la operadora británica BRITISH TELECOMMUNICATIONS PLC.
2. Mediante correo electrónico de fecha 23/11/2013 el Information Commissioner's Office, autoridad de protección de datos del Reino Unido, informó a esta Agencia que no tiene competencias para requerir información acerca de las IP a los proveedores de servicios de Internet.

FUNDAMENTOS DE DERECHO

I

La competencia para sancionar por la comisión de las infracciones tipificadas en el artículo 38.4.d) de la LSSI, corresponde a la Agencia Española de Protección de Datos según dispone el artículo 43.1 de dicha Ley.

II

Actualmente se denomina "*spam*" a todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo se entiende por "*spam*" cualquier mensaje no solicitado y que, normalmente, tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede

hacer por distintas vías, la más utilizada entre el público en general es el correo electrónico.

Esta conducta es particularmente grave cuando se realiza en forma masiva. El envío de mensajes comerciales sin el consentimiento previo está prohibido por la legislación española, tanto por la LSSI (a consecuencia de la transposición de la Directiva 2000/31/CE, de 8 de junio) como por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

El bajo coste de los envíos de correos electrónicos vía Internet o mediante telefonía móvil (SMS y MMS), su posible anonimato, la velocidad con que llega a los destinatarios y las posibilidades que ofrece en cuanto al volumen de las transmisiones, han permitido que esta práctica se realice de forma abusiva e indiscriminada.

La LSSI, en su artículo 21.1, prohíbe de forma expresa *“el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas”*. Es decir, se desautorizan las comunicaciones comerciales dirigidas a la promoción directa o indirecta de los bienes y servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, si bien esta prohibición encuentra la excepción en el segundo párrafo del citado artículo, que autoriza el envío cuando *“el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que fueron objeto de contratación”*. De este modo, el envío de comunicaciones comerciales no solicitadas, fuera del supuesto excepcional del art. 21,2 de la LSSI, puede constituir una infracción leve o grave de la LSSI.

Como ya se ha señalado en cuanto a la posible obtención ilícita de los datos del destinatario, la práctica del *“spam”* además de suponer una infracción a la LSSI, puede significar una vulneración de la legislación sobre protección de datos, ya que hay que tener en cuenta que la dirección de correo electrónico puede ser considerada como dato de carácter personal.

La Directiva sobre Privacidad en las Telecomunicaciones, de 12/07/02, (Directiva 2002/58/CE) transpuesta en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que modifica varios artículos de la LSSI, introdujo en el conjunto de la Unión Europea el principio de *“opt in”*, es decir, la necesidad de contar con el consentimiento previo del destinatario para el envío de correo electrónico con fines comerciales. De este modo, cualquier envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente queda supeditado a la prestación previa del consentimiento, salvo que exista una relación contractual anterior y el sujeto no manifieste su voluntad en contra.

Por lo tanto, atendiendo al enunciado del art. 21.1 de la LSSI, resulta esencial delimitar el sentido aplicado por la citada normativa a la exigencia de consentimiento, previo y expresamente manifestado por el destinatario del mensaje, para que pueda admitirse el envío de comunicaciones publicitarias o promocionales por correo electrónico.

La repetida LSSI, que tiene por objeto, entre otras materias, la regulación del envío de las comunicaciones comerciales por vía electrónica, establece expresamente en su artículo 1.2 que las disposiciones contenidas en la misma se entenderán sin perjuicio de lo dispuesto en las normas que tengan como finalidad la protección de datos personales.

Al referirse en el Título III de la LSSI a las *“comunicaciones comerciales por vía electrónica”*, el artículo 19 de la LSSI declara igualmente aplicable la LOPD y su normativa de desarrollo, *“en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales”*. Esta rotunda previsión legal permite afirmar que, además de lo establecido en la LSSI, serán exigibles en el tratamiento de datos personales para la realización de comunicaciones comerciales por medios electrónicos el conjunto de principios, garantías y derechos contemplados en la normativa de protección de datos de carácter personal.

Por tanto, en relación al concepto de consentimiento del destinatario para el tratamiento de sus datos con la finalidad de enviarle comunicaciones comerciales por vía electrónica, es preciso considerar lo dispuesto en la normativa de protección de datos y, en concreto, el artículo 3.h) de la LOPD que establece:

“Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen”.

Por tanto, de acuerdo con dicha definición, el consentimiento, además de previo, específico e inequívoco, deberá ser informado. Y esta información deberá ser plena y exacta acerca del tipo de tratamiento y su finalidad, con advertencia sobre el derecho a denegar o retirar el consentimiento. Esta información así configurada debe tomarse como un presupuesto necesario para otorgar validez a la manifestación de voluntad del afectado.

III

Como ya se ha señalado, la LSSI prohíbe las comunicaciones comerciales no solicitadas, partiendo de un concepto de comunicación comercial que se califica como servicio de la sociedad de la información y que se define en su Anexo de la siguiente manera:

“f) Comunicación comercial»: toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa,

organización o persona que realice una actividad comercial, industrial, artesanal o profesional.

A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica”.

Por su parte el Anexo a) de la citada LSSI reconoce como Servicios de la Sociedad de la Información, entre otros y siempre que representen una actividad económica, los envíos de comunicaciones comerciales.

De acuerdo con lo señalado, es preciso analizar el concepto de Servicios de la Sociedad de la Información para, a continuación, determinar los supuestos, recogidos en el párrafo segundo del Anexo f) de la LSSI, que no se consideran, a los efectos de esta Ley, como comunicaciones comerciales.

La LSSI en su Anexo a) define como Servicio de la Sociedad de la Información, *“todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario”*. A través de dicha definición el Legislador español transpuso el concepto recogido en las Directivas 98/34/CEE, de 22 de junio, del Parlamento y del Consejo, por la que se establece un procedimiento de información en materia de normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la Sociedad de la Información, modificada por la Directiva 98/84/CE, de 20 de noviembre, del Parlamento y del Consejo, relativa a la protección jurídica de los servicios de acceso condicional o basados en dicho acceso. Dicha definición se refiere, tal y como se expresa en el Considerando 17 de la citada Directiva 2000/31/CE, a *“cualquier servicio prestado normalmente a título oneroso, a distancia, mediante un equipo electrónico para el tratamiento (incluida la comprensión digital) y el almacenamiento de datos, y a petición individual de un receptor de un servicio”*, añadiendo que estos servicios cuando *“no implica tratamiento y almacenamiento de datos no están incluidos en la presente definición”*.

De acuerdo con lo señalado, el concepto de comunicaciones comercial engloba la definición recogida en el Anexo f), párrafo primero de la LSSI, es decir, ha de tratarse de todas las formas de comunicaciones destinadas a promocionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o profesional, y, además, ha de realizarse dicha comunicación en los términos que señala el Considerando 17 de la Directiva 2000/31/CE que recoge lo previsto en las citadas Directivas 98/34/CE y 98/84/CE.

De lo anterior se deduce que, cuando la comunicación comercial no reúne los requisitos que requiere el concepto de Servicios de la Sociedad de la Información, pierde el carácter de comunicación comercial. En este sentido el párrafo segundo del Anexo f) de la LSSI señala dos supuestos, que no tendrán, a los efectos de esta Ley, la consideración de comunicación comercial. Por un lado, los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, y, por otro, las comunicaciones

relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica.

IV

En el caso que nos ocupa, es de destacar lo señalado en el Informe de Actuaciones Previas de Inspección en el punto 1.e), que señala lo siguiente: “*De las consultas realizadas al DNS se encuentra que la dirección IP origen del mensaje está radicada en Reino Unido y pertenece a la operadora británica BRITISH TELECOMMUNICATIONS PLC*”. Por este motivo, se solicita a la autoridad de protección de datos del Reino Unido colaboración, contestando a esta Agencia que no tiene competencias para requerir información acerca de las IP a los proveedores de servicios de Internet.

En este orden de ideas, debe tenerse en cuenta que en el ámbito administrativo sancionador son de aplicación, con alguna matización pero sin excepciones, los principios inspiradores del orden penal, resultando clara la plena virtualidad de los principios de presunción de inocencia. La presunción de inocencia debe regir sin excepciones en el ordenamiento sancionador y ha de ser respetada en la imposición de cualesquiera sanciones, pues el ejercicio del *ius puniendi* en sus diversas manifestaciones está condicionado al juego de la prueba y a un procedimiento contradictorio en el que puedan defenderse las propias posiciones. En tal sentido, el Tribunal Constitucional, en Sentencia 76/1990 considera que el derecho a la presunción de inocencia comporta “*que la sanción esté basada en actos o medios probatorios de cargo o incriminadores de la conducta reprochada; que la carga de la prueba corresponda a quien acusa, sin que nadie esté obligado a probar su propia inocencia; y que cualquier insuficiencia en el resultado de las pruebas practicadas, libremente valorado por el órgano sancionador, debe traducirse en un pronunciamiento absolutorio*”. De acuerdo con este planteamiento, el artículo 130.1 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común en lo sucesivo LRJPAC), establece que “*Sólo podrán ser sancionados por hechos constitutivos de infracción administrativa las personas físicas y jurídicas que resulten responsables de los mismos aún a título de simple inobservancia.*”

Conforme señala el Tribunal Supremo (STS 26/10/98) el derecho a la presunción de inocencia “*no se opone a que la convicción judicial en un proceso pueda formarse sobre la base de una prueba indiciaria, pero para que esta prueba pueda desvirtuar dicha presunción debe satisfacer las siguientes exigencias constitucionales: los indicios han de estar plenamente probados – no puede tratarse de meras sospechas – y tiene que explicitar el razonamiento en virtud del cual, partiendo de los indicios probados, ha llegado a la conclusión de que el imputado realizó la conducta infractora, pues, de otro modo, ni la subsunción estaría fundada en Derecho ni habría manera de determinar si el proceso deductivo es arbitrario, irracional o absurdo, es decir, si se ha vulnerado el*

derecho a la presunción de inocencia al estimar que la actividad probatoria pueda entenderse de cargo.”

La Sentencia del Tribunal Constitucional de 20/02/1989 indica que *“Nuestra doctrina y jurisprudencia penal han venido sosteniendo que, aunque ambos puedan considerarse como manifestaciones de un genérico favor rei, existe una diferencia sustancial entre el derecho a la presunción de inocencia, que desenvuelve su eficacia cuando existe una falta absoluta de pruebas o cuando las practicadas no reúnen las garantías procesales y el principio jurisprudencial in dubio pro reo que pertenece al momento de la valoración o apreciación probatoria, y que ha de juzgar cuando, concurre aquella actividad probatoria indispensable, exista una duda racional sobre la real concurrencia de los elementos objetivos y subjetivos que integran el tipo penal de que se trate.”*

En definitiva, aquellos principios impiden imputar una infracción administrativa cuando no se haya obtenido y constatado una prueba de cargo acreditativa de los hechos que motivan esta imputación o de la intervención en los mismos del presunto infractor, aplicando este principio en caso de duda respecto de un hecho concreto y determinante, que obliga en todo caso a resolver dicha duda del modo más favorable al interesado.

En este caso, procede resaltar, junto con la presunción de inocencia de todo imputado, que no se ha podido determinar la presunta entidad responsable debido a que se desconoce el titular de la dirección IP objeto de los correos.

V

Por lo tanto no se puede advertir conducta alguna que encaje en el catalogo de infracciones que la LSSI establece en su Titulo VII, procediendo el archivo de las presentes actuaciones.

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 **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 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.