AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

GUÍA PARA LA LUCHA CONTRA EL SPAM

Agencia Española de Protección de Datos

ÍNDICE

I.- ¿Qué es el Spam?

Actualmente se denomina Spam o "correo basura" 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 mediante 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 Ley 34/2002 de Servicios de la Sociedad de la Información (a consecuencia de la transposición de la Directiva 31/2000/CE) como por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos.

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

La Ley de Servicios de la Sociedad de la Información, 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 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 artículo, que autoriza el envío cuando exista una relación contractual previa y se refiera a productos similares. De este

modo, el envío de comunicaciones comerciales no solicitadas puede constituir una infracción leve o grave de la LSSI.

Además de suponer una infracción a la Ley de Servicios de la Sociedad de la Información, la práctica del Spam puede significar una vulneración del derecho a la intimidad y el incumplimiento 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 de julio de 2002 (Directiva 58/2002/CE) actualmente transpuesta en la Ley 32/2003 General de Telecomunicaciones que modifica varios artículos de la Ley 34/2002 introdujo en el conjunto de la Unión Europea el principio de "*opt in*", es decir, el consentimiento previo de la persona para el envío de correo electrónico con fines comerciales. De este modo, cualquier envío con fines de publicidad queda supeditado a la prestación del consentimiento, salvo que exista una relación contractual previa y el sujeto no manifieste su voluntad en contra.

II.-Formas de Spam

- Correo electrónico

Debido a la facilidad, rapidez y capacidad en las transmisiones de datos, la recepción de comunicaciones comerciales a través de este servicio de la sociedad de la información es la más usual, y el medio por el que los *spammers* envían más publicidad no deseada.

- Spam por ventanas emergentes (Pop ups)

Se trata de enviar un mensaje no solicitado que emerge cuando nos conectamos a Internet. Aparece en forma de una ventana de diálogo y advertencia del sistema Windows titulado "servicio de visualización de los mensajes". Su contenido es variable, pero generalmente se trata de un mensaje de carácter publicitario.

Para ello se utiliza una funcionalidad del sistema de explotación Windows, disponible sobre las versiones Windows NT4, 2000, y XP y que permite a un administrador de redes enviar mensajes a otros puestos de la red.

La solución más sencilla para evitar estas ventanas emergentes consiste en desactivar este servicio de Windows. Otro método consiste en utilizar un cortafuegos destinado a filtrar los puertos TCP y UDP (135, 137,138, 139 y 445) de su ordenador, pero con esta medida es posible que deje de funcionar la red.

- Phising

No es exactamente una modalidad de Spam, más bien una técnica de ingeniería social para recolectar datos de forma fraudulenta.

El *Phising* es la duplicación de una página web para hacer creer al visitante que se encuentra en la página original en lugar de en la ilícita. Se suele utilizar con fines delictivos duplicando páginas web de bancos y enviando indiscriminadamente correos mediante Spam para que se acceda a esta página con el fin de actualizar los datos de acceso al banco, como contraseñas, fechas de caducidad, etc.

- Hoax

El *hoax* es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena.

Algunos hoax informan sobre virus, otros invocan a la solidaridad, o contienen fórmulas para ganar millones o crean cadenas de la suerte.

Los objetivos que persigue quien inicia un hoax son normalmente captar direcciones de correo o saturar la red o los servidores de correo.

- Scam

El *Scam* no tiene carácter de comunicación comercial. Este tipo de comunicación no deseada implica un fraude por medios telemáticos, bien vía teléfono móvil o por correo electrónico.

- Spam en el móvil

Además de las comunicaciones del operador de telefonía mediante mensajes de texto (SMS- *Short Message Services*), o mensajes multimedia (MMS- *Multimedia Message Services*), existen otro tipo de comunicaciones publicitarias en las que no media un consentimiento previo ni una relación contractual, por lo que son consideradas comunicaciones comerciales no solicitadas.

Este tipo de comunicaciones generan un gasto de tiempo y de dinero. Además los MMS pueden introducir virus y explotar de forma maliciosa alguna vulnerabilidad de los sistemas internos del teléfono.

- Comunicaciones comerciales no solicitadas en el fax o llamadas sin intervención humana

Aunque este tipo de envíos no están considerados en principio como Spam, también son sancionables por la Agencia Española de Protección de Datos, aplicándose las mismas multas que la ley establece para el Spam.

III.-Consejos para prevenir el Spam

La dirección de correo electrónico es el medio más utilizado para registrar la identidad de una persona en Internet y suele servir de base para la acumulación de información en torno a la misma. En muchas ocasiones contiene información acerca de la persona como el apellido, la empresa donde trabaja o el país de residencia. Esta dirección puede utilizarse en múltiples lugares de la red y puede ser conseguida fácilmente sin nuestro conocimiento, por lo que es necesario seguir una serie de normas para salvaguardar nuestra privacidad.

- Ser cuidadoso al facilitar la dirección de correo

Facilitar únicamente la dirección de correo a aquellas personas y organizaciones en las que confía y aquellas con las que quiera comunicar.

- Utilizar dos o más direcciones de correo electrónico

Es aconsejable crear una dirección de correo electrónica, que será la que se debe proporcionar en aquellos casos en los que no se confíe o conozca lo suficiente al destinatario. De este modo, su dirección personal será conocida únicamente por sus amigos o por sus contactos profesionales, con el ahorro de tiempo que implica no tener que separar correos importantes de aquellos no deseados.

Lo mismo se recomienda a la hora de utilizar servicios de mensajería instantánea.

- Elegir una dirección de correo poco identificable.

Los *spammers* obtienen las direcciones de correo electrónico de formas muy diferentes. Así navegando por la red, en salas de chat e IRC, o incluso en directorios de contactos o usando la ingeniería social. A veces compran incluso listas de correo electrónico en sitios web que venden los datos de sus clientes. Y, cuando todo esto falla, simplemente conjeturan.

Las direcciones de correo electrónico que se refieren a una persona como tal, suelen contener algún elemento que les identifique y son fáciles de recordar.

Esta forma de crear el correo permite a los *spammers* intuir las direcciones de correo electrónico. Por ejemplo, si su nombre es Jesús Fernández, el spammer probará con las siguientes opciones: jesusfernandez@...., j.fernandez@...., jfdez@....., jesus.fdez@...., etc.

Los *spammers* incluso cuentan con programas que generan automáticamente posibles direcciones de correo. Pueden crear cientos de direcciones en un minuto, ya que trabajan utilizando diccionarios, es decir, una lista de palabras que se suelen usar en las direcciones de correo. Estos diccionarios suelen contener campos como los siguientes:

- Alias
- Apellidos
- Iniciales
- Apodos
- Nombres de mascotas
- Marcas
- Signos del zodiaco
- Meses del año
- Días de la semana
- Nombres de lugares
- Modelos de coches
- Términos deportivos
- Etc.

Estos programas simplemente introducen datos en cada uno de estos campos e intentan varias combinaciones con todos ellos. Además añaden letras y números en las combinaciones, ya que se suelen introducir fechas de cumpleaños, edades, etc.

Para crear una dirección de correo electrónico y reducir el envío de Spam, sería conveniente no introducir campos que sean potencialmente intuíbles por el *spammer*.

-No publicar la dirección de correo

No se debería anunciar la dirección de correo en buscadores, directorios de contactos, foros o páginas web. En el caso de los chat, no se debe mostrar la dirección de correo electrónico en las listas de usuarios y no se debe comunicar a desconocidos.

Cuando envíe correos en los que aparezcan muchas direcciones, envíelas usando BCC o CCO (con copia oculta) para no hacer visibles todas las direcciones.

Si es necesario facilitar la dirección de correo electrónico en alguna web, envíela en formato imagen o escriba 'at' o 'arroba' en lugar de @. De este modo se puede evitar que lo capturen los programas creadores de Spam. Asimismo, si reenvía un correo, elimine las direcciones de los anteriores destinatarios: son datos de fácil obtención por los *spammers*.

- Leer detenidamente las Políticas de Privacidad y las Condiciones de Cancelación.

Si se va a suscribir a un servicio *on line*, o a contratar un producto, revise la política de privacidad antes de dar su dirección de correo electrónico u otra información de carácter personal. Puede que esta compañía vaya a ceder los datos a otras o a sus filiales y observe que no le suscriben a boletines comerciales, por lo que es conveniente saber la política de alquiler, venta o intercambio de datos que han adoptado tanto su proveedor de acceso a Internet como los administradores de los directorios y listas de distribución donde esté incluido. Capture la pantalla y páginas en las que compra y conserve los datos identificadores.

Además, lea los mensajes sospechosos como texto y no como html y desactive la previsualización de los correos.

No dude en ejercer los derechos de acceso y cancelación sobre sus datos ante estas empresas.

-Sensibilizar a los niños sobre la utilización del correo y la mensajería instantánea

Los niños son objetivos ideales para promocionar información sobre la composición y las prácticas de consumo del hogar. Por eso es importante recordarles algunos consejos prácticos que ayudarán a evitar que el niño aporte datos personales.

Además, mediante la dirección de correo electrónico no se puede saber quien es el destinatario de correos que pueden tener contenidos no aptos para los niños.

IV.- Consejos para reducir el Spam

¿Qué hacer si ya recibe Spam?

Una vez que se empieza a recibir Spam, es casi imposible detenerlo completamente sin recurrir a un cambio de dirección de correo electrónico.

De todas formas, se recogen una serie de recomendaciones que pueden ser aplicados para reducir la proliferación del "correo basura".

- No es conveniente contestar al Spam

La Ley 34/2002 en su artículo 21.2 prevé que aquellos que realicen envíos electrónicos publicitarios han de habilitar procedimientos sencillos y gratuitos para que los destinatarios puedan solicitar no recibir más mensajes. Sin embargo, debe tenerse en cuenta que la mayoría de los correos basura que se reciben proceden de fuera de nuestras fronteras, y no están sujetos por tanto a nuestra legislación. Responder a dichos correos informa al remitente de que la dirección está activa, lo que puede animar tanto a ése como a otros *spammers* a enviar todavía más mensajes. Sólo se deben responder, de entre los correos electrónicos que reciba desde fuera de España, aquellos de los que conozca el remitente y confíe en él.

Es conveniente desactivar la opción que envía un acuse de recibo al remitente de los mensajes leídos del sistema de correo electrónico. Si un *spammer* recibe dicho acuse sabrá que la dirección está activa, y lo más probable es que le envíe más Spam.

- No pinche sobre los anuncios de los correos basura.

Entrando en las páginas web de los *spammers* podemos demostrar que nuestra cuenta de correo está activa, con lo que puede convertirse en un objetivo para nuevos envíos. Por otra parte, los gráficos e imágenes (también llamados *web bugs* –incluidos en los correos basura pueden proporcionar al *spammer* no sólo la información de que el mensaje ha sido recibido, sino también datos de carácter personal como la dirección IP.

- Utilice filtros de correo

- Programas de filtrado de correo electrónico.

Los programas de gestión de correo electrónico, así como muchas páginas web de correo, ofrecen la posibilidad de activar filtros que separan el correo deseado del Spam. Las principales desventajas son que puede confundir correos legítimos con mensajes basura. Cada vez se fabrican programas más avanzados en este campo, que en muchos casos pueden ser descargados libremente de Internet. Estos filtros reciben instrucciones para definir que tipo de correos se quiere recibir y cuales son considerados como Spam.

- Filtros basados en ISP

Muchos proveedores de Internet ofrecen soluciones que pueden llegar a ser muy efectivas a la hora de bloquear el Spam. Utilizan combinaciones de listas negras y escaneado de contenidos para limitar la cantidad de Spam que llega a las direcciones. El principal inconveniente es que, en ocasiones, bloquean correos legítimos, y además suelen ser servicios de pago. Para más información, consulte con su proveedor.

-Mantenga al día su sistema

Los ordenadores personales requieren de un mantenimiento. La mayoría de las compañías de software distribuyen actualizaciones y parches de sus productos que corrigen los problemas detectados en sus programas.

Estas actualizaciones suelen estar disponibles en las páginas web de los fabricantes, y generalmente su descarga e instalación es gratuita. Por otra parte, los usuarios deberían utilizar programas **antivirus** para protegerse contra estos perniciosos programas, capaces de destruir todos los archivos de un ordenador, y que cada vez son más utilizados por los *spammers*.

Asimismo, es muy recomendable la instalación de un **cortafuegos** para monitorizar lo que ocurre en el ordenador.

-Consulte nuestra guía de Recomendaciones para Usuarios de Internet

En estas recomendaciones se describen los principales servicios de Internet, la identificación de los posibles riesgos para la privacidad que su uso puede ocasionar y los consejos que se proponen a los usuarios.

V.- Legislación y textos de interés

Las leyes que regulan el envío no solicitado de comunicaciones comerciales electrónicas son, por un lado la **Ley 34/2002 de Servicios de la Sociedad de la Información** y por otro, la **Ley 32/2003 General de Telecomunicaciones**.

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (LGT), y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI), otorgan competencias a la Agencia Española de Protección de Datos.

La Ley General de Telecomunicaciones concede a la Agencia la tutela de los derechos y garantías de abonados y usuarios en el ámbito de las comunicaciones electrónicas, delegando en ella la imposición de sanciones por vulneración en la prestación de los servicios de comunicaciones electrónicas.

Por otro lado, la citada Ley de Servicios de la Sociedad de la Información establece que corresponde a la AEPD la imposición de sanciones en el caso de infracción por la remisión de comunicaciones comerciales no solicitadas efectuadas a través de correo electrónico o medios de comunicación electrónica equivalentes, sin cumplir las previsiones estipuladas en su articulado.

-Artículos relativos al envío de comunicaciones electrónicas en la LSSI.

Los artículos relativos al envío de comunicaciones no solicitadas por Internet son los siguientes: 19, 20, 21, 22, 38 y 43.

- Artículos de la Ley Orgánica de Protección de Datos.

Los artículos relevantes en la LOPD son los siguientes: 3.a), 4, 5, 6, 37.1.n) y 44 y 45.

- Artículos de la Ley General de Telecomunicaciones.

Artículos 38, 53.z, 54.r, 58.b y Disposición Adicional Novena de la Ley 32/2003.

- Otros textos legales de interés.

- Directiva 1995/46/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 (Directiva sobre Protección de Datos).

- Directiva 2000/31/CE, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el Comercio Electrónico).

- Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

-Documentos del Grupo del Artículo 29

- Dictamen 7/2000 sobre la propuesta de la Comisión Europea de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas de 12 de julio de 2000 COM (2000) 385. Adoptado el 2 de noviembre de 2000 (WP 36).

- Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE. Adoptado el 27 de febrero de 2004 (WP 90).

- Otros Textos

- Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones comerciales no solicitadas o Spam**.** Bruselas, 22.01.2004

-Comisión de las Comunidades Europeas. Comunicaciones comerciales no solicitadas y protección de datos. Resumen de las conclusiones del estudio. Enero de 2001.

VI.- Competencias de la Agencia Española de Protección de Datos

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (LGT), y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI), modificada por la LGT y por la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, ampliaron las competencias de la Agencia Española de Protección de Datos.

La Ley General de Telecomunicaciones atribuye a la Agencia la tutela de los derechos y garantías de abonados *(persona física o jurídica con contrato con el operador)* y usuarios *(quienes utilizan los servicios sin haberlos contratado)* en el ámbito de las comunicaciones electrónicas, encomendándole la imposición de sanciones por vulneración en la prestación de los servicios de comunicaciones electrónicas de los siguientes derechos:

- A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio o para que el operador pueda exigir su pago.

- A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello.

- A recibir facturas no desglosadas cuando así lo solicitasen (*).

- A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.

- A detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero (*).

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere.

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea al usuario que le realice una llamada (*).

- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada (*).

- A no recibir llamadas automáticas sin intervención humana o mensajes de fax, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.

- Además se garantizará a los abonados el derecho a no figurar en las guías ni en los servicios que informan sobre ellos. De este modo, se requerirá el consentimiento expreso para la inclusión por primera vez de datos en las citadas guías, y el consentimiento tácito para las sucesivas publicaciones. No obstante, y en relación con datos incluidos en la guía ya existente a que se refiere el artículo 30 del RD 424/2005, bastará con que tras la recepción de la comunicación que recibirá solicitándole si quiere mantener sus datos en la guía, el abonado no se oponga expresamente a dicha inclusión en el plazo de un mes. Para la inclusión de más datos de los mencionados en el artículo 30* del RD 424/2005 se exigirá el consentimiento expreso, tanto para la primera vez como para las sucesivas.

** Debe figurar, al menos, la siguiente información: a) Nombre y apellidos, o razón social. b) Número o números de abonado. c) Dirección postal del domicilio, excepto piso, letra y escalera. d) Terminal específico que deseen declarar, en su caso. e) Nombre del operador que facilite el acceso a la red.*

(*) *Estos derechos sólo están reconocidos por la LGT para los abonados a servicios de comunicaciones electrónicas.*

La **Ley de Servicios de la Sociedad de la Información** establece que corresponde a la Agencia, la imposición de sanciones en el caso de infracciones por el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes, sin cumplir las siguientes previsiones:

- Queda prohibido 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, **salvo** que exista una **relación contractual previa**, siempre que 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 inicialmente fueron objeto de contratación con el cliente.

> (*) *En cualquier caso, el prestador deberá ofrecer al destinatario la **posibilidad de oponerse** al tratamiento de sus datos con fines promocionales mediante un **procedimiento sencillo y gratuito**, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.*

El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente. A tal efecto, los prestadores de servicios deberán habilitar **procedimientos sencillos y gratuitos para** que los destinatarios de servicios puedan **revocar** el consentimiento que hubieran prestado, y deberán **facilitar información** accesible por medios electrónicos **sobre dichos procedimientos**.

- Cuando los prestadores de servicios empleen **dispositivos de almacenamiento y recuperación de datos en equipos terminales (cookies), informarán** a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la **posibilidad de rechazar el tratamiento** de los datos mediante un **procedimiento sencillo y gratuito**.

Lo anterior no impedirá **el posible almacenamiento o acceso** a datos con el fin de efectuar o facilitar técnicamente la **transmisión de una comunicación**

por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información **expresamente solicitado** por el destinatario.

> (*) *Esta previsión ha sido introducida por la LGT, encontrándose en vigor desde el día 5 de noviembre de 2003. Asimismo, esta ley ha endurecido el régimen de infracciones y sanciones previsto en la LSSI en aquellos casos en los que se produzcan envíos masivos de spam, o remisiones a un mismo destinatario, en el plazo de un año, de más de tres comunicaciones comerciales no deseadas por medios electrónicos.*

Las sanciones previstas en la Ley de Servicios de la Sociedad de la Información respecto del Spam son también aplicables cuando no se respeta el derecho de los abonados a no recibir llamadas automáticas sin intervención humana o mensajes de fax con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.

Investigar los casos de Spam se está convirtiendo en una tarea cada vez más complicada, en tanto en cuanto los *spammers* contratan piratas informáticos para ocultar su verdadera identidad (*spoofing*). Los proveedores de servicios de Internet (ISP) suelen ser diligentes a la hora de cortar el servicio a los *spammers* cuando constatan que se generan correos basura desde sus redes.

Si tiene conocimiento del país a partir del cual se emite el Spam, puede indicarlo a las autoridades interesadas. Tratándose de Spam emitido en un Estado de la Unión Europea, los datos del conjunto de las autoridades europeas de protección de datos están disponibles en la página web de la AEPD. Si el envío de Spam se ha realizado desde los Estados Unidos de Norteamérica, pueden transferir los mensajes no solicitados al Departamento del Comercio Americano (Federal Trade Commission) que propone un procedimiento de alerta en su página web www.ftc.gov y con el que la Agencia Española de Protección de Datos ha suscrito un Acuerdo de Colaboración.

En la sección Denuncias y Reclamaciones de nuestra página web encontrará información acerca de cómo presentar una denuncia ante la Agencia. Antes de poner en conocimiento de la AEPD un caso de Spam, asegúrese de que no se trata de una comunicación comercial solicitada.

A continuación encontrará las direcciones web de los organismos homólogos de la Agencia Española de Protección de Datos, muchos de ellos con competencia en la lucha anti spam.

Austria: Austrian Data Protection Authority
Bélgica: Privacy Protection Commission
Chipre: Office of the Commissioner for Personal Data Protection.
Dinamarca: Danish Consumer Ombudsman
Eslovaquia: Slovak Personal Data Protection
Estonia: Estonian Data Protection Inspectorate
Finlandia: Data Protection Ombudsman
Francia: Commission Nationale de l'informatique et des Libertés (CNIL)
Grecia: Hellenic Data Protection Authoritie
Hungría: Data Protection and Freedom of Information Commissioner of Hungary
Irlanda: Data Protection Commissioner
Italia: Garante per la protezione dei dati personali
Letonia: Datu valsts inspekcijas
Lituania: Valstybinė duomenų apsaugos inspekcija
Luxemburgo: Commission nationale pour la protection des données
Malta: Data Protection Commissioner
Paises Bajos: College bescherming persoonsgegevens
Polonia: Inspector General for the Protection of Personal Data
Portugal: Comissão Nacional de Protecção de Dados
República Checa: Office for Personal Data Protection
Suecia: Swedish Data Inspection Board

VII.- Soluciones internacionales a un problema internacional

Desde que, en 2003, la Agencia Española de Protección de Datos se encarga de velar por el cumplimiento de la Ley de Servicios de la Sociedad de la Información y la Ley General de Telecomunicaciones, otorgándosele la misión competencial de supervisión en materia de comunicaciones comerciales no solicitadas (Spam), se ha ampliado y promovido su actividad internacional, ya que en virtud del artículo 37.1 de la LOPD este organismo debe ejercer la cooperación internacional necesaria para cumplir las funciones que le han sido encomendadas.

Efectivamente el problema del Spam, por la propia naturaleza de Internet y la evolución tecnológica de los medios a través de los cuales se produce, es un problema eminentemente internacional frente al que hay que actuar con medidas de participación internacional, sincronizadas y adoptadas conjuntamente por todos los implicados, de acuerdo con todas las legislaciones, que en ocasiones no regulan esta materia de una misma forma.

Para la consecución de esta cooperación internacional se han firmado varios documentos de colaboración y asistencia recíproca con las instituciones que tienen encomendada esa función de supervisión en diferentes países, tanto a nivel comunitario como extracomunitario.

- Relaciones con Europa

En el ámbito intraeuropeo, la Agencia Española de Protección de Datos forma parte del grupo ***Contact Network of Spam Authorities*** (CNSA). Este grupo está compuesto por las Autoridades nacionales responsables de la regulación y control de las comunicaciones no solicitadas de la Unión Europea y del Espacio Económico Europeo. En la última reunión celebrada en Bruselas se acordó la redacción de un documento con el objetivo de establecer un marco intraeuropeo para el intercambio de información sobre denuncias sobre Spam entre autoridades competentes, con indicaciones claras sobre lo que hay que

hacer cuando se recibe una denuncia. El punto común de estos países es el artículo 13 de la Directiva 2002/58/CE.

Dicho documento se aprobó en diciembre de 2004 y en el mismo se establece un procedimiento de cooperación en la transmisión de información referente a la aplicación del artículo 13 de la Directiva 2002/58/CE o de cualquier otra legislación nacional aplicable que se refiera a las comunicaciones comerciales no solicitadas.

En virtud de este acuerdo, se aprobaron las siguientes formas de colaboración:

- Al recibir una queja internacional, y antes de remitirlo a la Autoridad Nacional Competente, la Autoridad Nacional ha de verificar que la denuncia es viable y que se trata de una persona física. Asimismo se ha de informar al denunciante de la cesión de sus datos personales a otra Autoridad. Las diferentes autoridades que tengan información sobre la contravención de la normativa sobre Spam en otra jurisdicción nacional, compartirán dicha información con la Autoridad competente.

- Establecer el marco de cooperación entre autoridades y el reparto de las denuncias.

- Mantener el secreto de las informaciones y denuncias, eliminando cualquier información sensible que haya comunicado una Autoridad a otra, de acuerdo a la legislación nacional aplicable.

- Este texto no es vinculante sobre las legislaciones nacionales o internacionales.

- Relaciones con Estados Unidos.

Con esta idea de cooperación global, se ha firmado con la Comisión Federal del Comercio de los Estados Unidos (Federal Trade Commission– FTC) un Acuerdo de Cooperación Administrativa para luchar contra el Spam- **Memorando Of Understanding** (MOU)-, organismo federal con competencias supervisoras y de control en los Estados Unidos. En virtud de este Convenio ambas partes acuerdan las siguientes formas de colaboración:

- Facilitar la formación de usuarios y empresas en relación con el Spam.

- Promover códigos de conducta sobre buenas prácticas.

- Intercambiar información sobre las soluciones técnicas más avanzadas y mantenerse informados de las novedades;

- Colaborar con las universidades de los respectivos países para promover la investigación, conferencias y cursos formativos sobre la materia;

- Prestarse asistencia mutua en sus investigaciones.

La lucha contra el Spam en los Estados Unidos parte de una realidad normativa muy distinta a la europea. Básicamente, en este país se establece un sistema de *opt-out* en la Ley que regula este tipo de comunicaciones, la "CAN-SPAM Act".

- Relaciones multilaterales.

La AEPD ha participado en grupos de trabajo multilaterales contra el Spam y con esta finalidad se reunió en Londres en octubre de 2004, junto con otros responsables mundiales de la lucha contra Spam (agencias independientes y ministerios responsables) y sectores industriales implicados.

En este grupo de trabajo se reunieron los presidentes de la Comisión Federal de Comercio de los Estados Unidos (*Federal Trade Commission*- FTC), de la Comisión de Información del Reino Unido, de la Comisión de Libre Comercio del Reino Unido, la Comisión Nacional de Libertades e Información de Francia, el Regulador de las Telecomunicaciones de Países Bajos, el Director de la Oficina Australiana de Defensa del Consumidor y Competencia, el Director de la Agencia Española de Protección de Datos y el responsable internacional de la FTC.

Fruto de esta reunión se redactó una declaración final para iniciar un plan conjunto de actuación conocido como "**London Action Plan**" (LAP), que fue suscrito por 19 organismos e instituciones procedentes de 15 países distintos.

El LAP tiene por objeto desarrollar contactos internacionales para investigar casos de Spam y todos aquellos problemas conexos con el mismo. Los suscriptores del LAP hemos sido mayoritariamente Agencias y Comisiones Nacionales, y hemos asumido los compromisos suficientes para:

- Impulsar y favorecer la comunicación entre nosotros para supervisar más eficazmente el cumplimiento de la ley.

- Organizar conferencias periódicas para debatir: casos, desarrollos normativos, investigaciones, nuevas técnicas y formas de eliminar obstáculos en la investigación de casos de Spam. Informar y educar a los usuarios y consumidores.

- Favorecer el dialogo con las agencias públicas y el sector privado para actuar conjuntamente e impulsar iniciativas de cooperación.

- Relaciones con Iberoamérica.

La Agencia también ha querido fortalecer los lazos y fijar posiciones comunes en torno a la protección de datos personales en los países de Iberoamérica y para ello participó muy activamente, en el año 2004, en el **III Encuentro Iberoamericano**, que se celebró en Cartagena de Indias (Colombia). Este encuentro, que contó con la colaboración de la Agencia Española de Cooperación Internacional (AECI) y la Fundación Internacional y para Iberoamérica de Políticas Públicas (FIIAPP), reunió a más de 40 autoridades y destacados representantes de la esfera pública y privada de 15 países Iberoamericanos (Argentina, Brasil, Chile, Costa Rica, Colombia, El Salvador, Ecuador, España, México, Nicaragua, Perú, Panamá, Portugal, Uruguay y Venezuela). Entre otros temas de esta reunión, se trataron los ataques a la privacidad en el sector de las telecomunicaciones e Internet y la lucha contra el Spam, acordándose las siguientes actuaciones:

-Fijar medidas técnicas y legislativas para evitar el Spam que disciplinen la lucha en este sentido.

-Promover una colaboración internacional, estableciendo un marco homogéneo.

-Propiciar iniciativas de autorregulación sectorial que complementen y faciliten la ampliación del marco regulatorio sobre la materia.

Fruto de este Encuentro se aprobaron unas conclusiones que se incluyen en la Declaración final aprobada (**Declaración de Cartagena de Indias**), que analizan y acercan enfoques comunes en torno a los grandes temas analizados.

Existen además **otros foros internacionales** en los que España participa y colabora activamente, como son los siguientes:

- ITU- Unión Internacional de Telecomunicaciones. Para saber más acerca de este foro, puede acceder a él mediante el siguiente hipervínculo.: http://www.itu.int/osg/spu/spam/. La UIT fue el organismo de las Naciones Unidas encargado de dirigir la organización de la Cumbre Mundial sobre la Sociedad de la Información. La Agencia ha participado en **Acciones de Cooperación Internacional** con el fin de generar confianza y seguridad en la utilización de las TIC. Además la Agencia trabaja en diversas iniciativas en la lucha contra el Spam.

- OECD Task Force. En este foro los objetivos van encaminados a dar una repuesta internacional en las distintas políticas y a coordinar la lucha contra el Spam, alentado y promoviendo medidas para combatir el Spam y códigos de buenas prácticas en el sector de la industria y negocio, así como facilitar la aplicación de las leyes fronterizas. Se celebró el pasado año un taller en Bruselas para combatir el Spam, en el que participaron tanto Autoridades de Regulación como representantes del sector privado, analizándose los aspectos técnicos y socioeconómicos del Spam. Para obtener más información puede seguir el siguiente Hipervínculo: **OECD Work on Spam**

VIII.- Glosario de términos de Spam

Acuse de recibo: Un tipo de mensaje que se envía para indicar que un correo ha llegado a su destino sin errores. Un acuse de recibo puede también ser negativo, es decir, indicar que un bloque de datos no ha llegado a su destino.

Antivirus: Programa de ordenador que permite detectar y eliminar virus informáticos.

Can-Spam Act: Ley federal por la que se encuadra la práctica del *spamming* en Estados Unidos, de 16 de diciembre de 2003 que entró en vigor el 1 de enero 2004. Este texto prevé un mecanismo de derecho de oposición (*opt out*). Este texto prohíbe explícitamente los mensajes engañosos (utilización de falsas direcciones de expedición o el hecho de camuflar la naturaleza del mensaje) y la publicidad falsa del contenido del mensaje. **Can-Spam Act** responde al acrónimo de "*Controlling the Assault of Non-Solicited Pornography and Marketing Act*".

Cookies: Conjunto de datos que envía un servidor Web a cualquier navegador que le visita, con información sobre la utilización que se ha realizado, por parte de dicho navegador, de las páginas del servidor, en cuanto a dirección IP del navegador, dirección de las páginas visitadas, dirección de la página desde la que se accede, fecha, hora, etc. Esta información se almacena en un fichero en el ordenador del usuario para ser utilizada en una próxima visita a dicho servidor. Además, existen servidores que restringen la utilización de determinadas funcionalidades de sus servicios o, incluso, deniegan el uso de los mismos si el usuario decide no aceptar la grabación o colocación de la cookie en su ordenador.

Cortafuegos: Sistema de seguridad que permite controlar las comunicaciones entre redes informáticas. Instalado entre Internet y una red local permite evitar en esta última accesos no autorizados, protegiendo con ello su información interna.

Dirección de correo electrónico o *e-mail*: Serie de caracteres, numéricos o alfanuméricos, que identifican un determinado recurso de forma única y

permiten acceder a él. La dirección de correo electrónico está considerada como dato personal, ya que puede permitir la identificación del usuario de la misma.

Filtros: Permiten ordenar el correo entrante basándose en una serie de reglas definidas previamente.

Hoax: Del inglés, engaño o bulo.

Https: Versión segura del protocolo http. El sistema HTTPS usa un cifrado basado en las *Secure Socket Layers* (SSL) para crear un canal más apropiado para el tráfico de información personal que el protocolo HTTP. Se utiliza normalmente por entidades bancarias, tiendas *on line*, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

IRC: Siglas de *Internet Relay Chat*, protocolo de comunicaciones que permite participar en conversaciones virtuales en tiempo real (véase Sala de Chat).

ISP: Proveedor de Servicios a Internet.

Lista negra: Mecanismo de control de identificación que permite diferenciar entre personas que pueden acceder a un determinado servicio de otros que, constando en dicha lista, no pueden acceder.

Opt-in: Sólo mediante la petición expresa del particular, se podrá enviar comunicaciones comerciales. Se prohíbe todo tipo de comunicación comercial no consentida. Este es el mecanismo adoptado por las últimas Directivas Europeas. La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 202, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, transpuesta a nuestro derecho interno por la Ley 32/2003 General de Telecomunicaciones.

Opt-out: Permite el envío libre de este tipo de comunicaciones siempre que permita al destinatario del mismo solicitar la exclusión de la lista de envíos. Esta era la antigua tendencia europea con respecto a la prestación del consentimiento, tal y como se preveía en la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de sociedad de la información

y en particular el comercio electrónico en el mercado interior. En Estados Unidos sigue siendo el sistema legislativo vigente.

Phishing: Es la contracción de "*password harvesting fishing*" (cosecha y pesca de contraseñas).

Red: Conjunto de máquinas conectadas para intercambiar información entre sí.

Sala de Chat: Lugar virtual de la red, llamado también canal, donde los usuarios se reúnen para charlar con otros que se encuentran en la misma sala.

Spam: Véase "Qué es Spam"

Spammer: La persona o compañía que realiza el envío de Spam.

Spamming lists: Listas comerciales. Listas de direcciones de correo para envío de publicidad de forma masiva.

Spoofing: Suplantación de la identidad de un tercero. Aunque puede producirse en diferentes entornos uno de los más habituales en los que aparece con frecuencia es en el envío masivo de Spam.

URL: El URL es la cadena de caracteres con la cual se asigna dirección única a cada uno de los recursos de información disponibles en Internet.

Virus informático: Programa de ordenador que puede infectar otros programas o modificarlos para incluir una copia de sí mismo. Los virus se propagan con distintos objetivos, normalmente con finalidades fraudulentas y realizando daños en los equipos informáticos.

Web bug: También se denominan "micro espías" o "pulgas" y son imágenes transparentes dentro de una página web o dentro de un correo electrónico con un tamaño de 1x1 pixeles. Al igual que ocurre con las *cookies*, se utilizan para obtener información acerca de los lectores de esas páginas o los usuarios de los correos, tales como la dirección IP de su ordenador, el tipo y versión de navegador del internauta, el sistema operativo, idioma, cuanta gente ha leído el correo, etc.