BLOQUE III: EL ABUSO POR EXCELENCIA DE LA PUBLICIDAD *ON LINE*: EL *SPAM*.

1. Introducción. El *spam*.

En este bloque del proyecto vamos a abordar el problema del *spam* profundidad, comenzando por exponer más detalladamente ante qué tipo de problema estamos y sus efectos. Posteriormente haremos un análisis desde distintos puntos de vista, y para finalizar, estudiaremos las medidas que se están tomando para combatirlo. En el bloque II de este trabajo ya tocamos ligeramente el tema, encuadrándolo dentro de las formas de publicidad abusiva mediante Internet. De hecho, desde nuestra opinión, se trata de la forma de publicidad que representa un mayor abuso.

1.1. Por qué tratar este tema.

No hay lugar a dudas de que, junto con los virus, el *spam* es en la actualidad uno de los principales problemas de Internet. Un porcentaje cada vez más alto de todos los mensajes de correo electrónico que se envían y reciben mediante Internet (a fecha de febrero de 2004 era del 62%[126]) son anuncios de Viagra, páginas pornográficas o programas informáticos con el precio muy rebajado, porque son "piratas". Esta tendencia, que los expertos predicen que aumentará espectacularmente durante este año, puede hacer que en un futuro próximo el número de usuarios del correo electrónico, tal y como hoy en día se concibe, decrezca en lugar de aumentar ya que se podría llegar incluso a inutilizar el servicio. Si a todo esto añadimos la actitud agresiva con la que actúan últimamente los *spammers*, que vienen utilizando virus para convertir las propias máquinas de los usuarios en emisoras de *spam*, y atacan a los proyectos que luchan contra el *spam*, tenemos ante nosotros un problema de gran envergadura y de difícil

[126] Cifras tomadas de un estudio realizado por la compañía Brightmail, consultar el apartado 2.1.3., "Cantidad de *spam* que circula en Internet.".

solución, que merece la pena analizar en profundidad, dado que hasta hace pocos meses era desconocido para el internauta medio no especializado.

Recientemente, un estudio llevado a cabo por la Trans Atlantic Consumer Dialogue[127] (TACD, que se autodefine como un foro de 65 entidades europeas y norteamericanas de defensa del consumidor) revelaba que el número de usuarios que realiza compras *on line* ha decrecido por miedo al *spam*, tendencia que puede agudizarse en un futuro. Y es que a los internautas les está haciendo cada vez menos gracia tener que dar su dirección de correo electrónico para registrarse en un sitio *web*, o para hacer una compra *on line*, sea en el sitio *web* que sea. Por tanto estos resultados ponen de manifiesto que el *spam* está provocando el freno de la confianza de los internautas y consumidores *on line* en el comercio electrónico, y en Internet en general. Esta es la segunda razón por la que incluir el análisis de este problema en el proyecto.

Por último, el *spam* es uno de los principales abusos del correo electrónico, y por tanto de Internet[128], que en este caso se usa como forma de promoción de negocios electrónicos (tema central de este trabajo).

En efecto, el *spam* representa un abuso por una parte en los receptores de los mensajes, que se ven afectados desde el punto de vista de costes económicos, al tener que hacer frente al gasto (en tiempo y dinero de la recepción de estos mensajes) lo quieran o no, así como de costes sociales. Las implicaciones en el ámbito social se derivan de la molestia y ofensa asociada a determinados contenidos y a la inhibición del derecho a publicar la propia dirección en medios como listas de noticias o páginas *web*, por ejemplo, por miedo a que sea capturada. Por tanto, el *spam* viola los derechos de los receptores por múltiples razones, entre ellas la intrusión y la violación de la intimidad.

Por otra parte, el *spam* también representa un problema para los PSIs implicados en proporcionar el servicio de correo electrónico, que se deriva del afronte de grandes gastos. Éstos vienen dados por el consumo extra de recursos informáticos, el ancho de banda requerido para el procesamiento y entrega de miles de mensajes, y sobre todo, por el tiempo adicional de personal dedicado a solucionar estos problemas en situaciones de saturación. En efecto, ellos deben hacer frente a la mayor parte del coste por una publicidad que sólo revierte inconvenientes tanto para ellos como para los usuarios.

1.2. Definición del spam.

En este proyecto, denominaremos *spam* o correo electrónico basura a las comunicaciones comerciales no solicitadas realizadas a través de correo electrónico u otros medios electrónicos equivalentes. También consideramos *spam* al envío masivo de mensajes no solicitados, sean o no comerciales, que inundan Internet con muchas copias del mismo mensaje con la intención de remitirlo de forma indiscriminada a quien no elegiría recibirlo. Es decir, consideramos *spam* a las comunicaciones comerciales no

[127] Dada la importancia que tienen los resultados que arroja este estudio, el cual se ha realizado a usuarios de 36 países, ha sido incluido como anexo a este trabajo para que pueda consultarse con facilidad.

[128] Esta opinión también es compartida por la organización RedIris, quien considera que el *spam* se encuentra entre los principales Abusos en el Correo Electrónico (ACE). En su página web (www.rediris.com), RedIris agrupa los Abusos en el Correo Electrónico (ACE) en cuatro tipos: difusión de contenido inadecuado, difusión a través de canales no autorizados, difusión masiva no autorizada, y ataques con objeto de imposibilitar o dificultar el servicio. El *spam* incurre en los tres últimos tipos de abusos.

solicitadas, sean de forma masiva o no, y a las comunicaciones masivas no solicitadas, sean o no de naturaleza comercial.

Las diferentes definiciones de *spam* que se dan por parte de los distintos organismos no siempre coinciden. A veces el *spam* no se ve únicamente como un fenómeno comercial, puesto que hay que tener en cuenta que otros abusos del correo electrónico son similares, y hasta en muchos casos se habla de *spam* cuando se quiere referir a toda forma de correo no solicitado. En otras ocasiones no se considera *spam* si el mensaje no ha sido enviado de forma masiva.

Si acudimos por ejemplo a la definición que se dio en el 105 Congreso de los Estados Unidos[129], se consideran mensajes electrónicos comerciales a aquellos que contienen anuncios para la venta de productos o servicios, que contienen un número de teléfono a través del cual se puede comunicar el usuario con la persona responsable de un anuncio o de la venta de un producto o servicio; o que promueve el uso de listas de Internet que contienen dichos anuncios. En esta definición se contempla cualquier uso comercial, no aludiendo si el mensaje se distribuye de forma masiva o no.

Abusos del correo electrónico[130].

A continuación describimos otros abusos del correo electrónico que no serán tratados en este trabajo, se sólo explican brevemente con el fin de clarificar un poco más la definición de *spam* efectuada al comienzo de este apartado. A estos usos indebidos del sistema es técnicamente incorrecto denominarlos *spam*, porque puede haber casos en los que actividades llevadas a cabo por los *spammers* no puedan encuadrarse en ellos, y viceversa. Expliquemos pues, cuales son estos abusos:

- **Difusión de contenido inadecuado**, es decir, contenido ilegal por su complicidad con hechos delictivos, como apología del terrorismo, programas "piratas", pornografía infantil, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o códigos maliciosos, etc. La temática del *spam* abarca en la mayoría de las ocasiones[131] casi todos los ejemplos comentados de contenido inadecuado.
- **Difusión a través de canales no autorizados**, es decir, usando estafetas ajenas para enviar correo propio. Aunque el mensaje sea legítimo, se están utilizando recursos ajenos sin consentimiento. Los *spammers* a menudo utilizan máquinas ajenas para hacer sus envíos.
- **Difusión masiva no autorizada**, que en inglés se conoce con las siglas UBE (*Unsolicited Bulk Email*). Es el uso de máquinas propias o ajenas para enviar de forma masiva cualquier tipo de correo no solicitado. Se trata de cualquier grupo de mensajes no solicitados, cuyo contenido es sustancialmente idéntico (muchos proveedores de servicio especifican un umbral para denominar envío masivo de 25 o

[129] La S 1618 ES, en su propuesta para el 105 Congreso de los Estados Unidos, en su sección 306 nos da una definición de lo que designamos "*spam mail*" o mensajes *spam*. La incluimos a continuación de forma textual:

The term "commercial electronic mail" means any electronic mail that:

a) Contains an advertisement for the sale of a product or service;

b) Contains a solicitation for the use of a telephone number, the use of which connects the user to a person or service that advertises the sale of or sells a product or service; or

c) *Promotes the use of or contains a list of one or more Internet sites that contain an advertisement referred to in subparagraph (a) or a solicitation referred to in subparagraph (b).*

[130] Las principales ideas sobre los tipos de abusos del correo electrónico se ha tomado del sitio web http://members.aol.com, y en concreto de la publicación "Email Abuse FAQ".

[131] Consultar el apartado 2.1.2.1., "Categorías de *spam*", en el que se dan cifras sobre los temas que abarca el *spam*.

más direcciones de destino en un periodo de 24 horas). Se considera un abuso por varios motivos, pero principalmente porque el emisor de los mensajes descarga en los transmisores y receptores el coste de sus operaciones, tanto si están de acuerdo con ello, como si no. El *spam* puede ser un caso particular de la difusión masiva no autorizada.

- **Comunicaciones comerciales no solicitadas**, que también son conocidas con las siglas inglesas UCE (*Unsolicitated Commercial Email*). Esto no implica que los envíos se realicen de forma masiva, pues el simple envío de un mensaje ya constituye una violación, y de hecho es ilegal en muchos países como España.
- **Ataques con objeto de imposibilitar o dificultar el servicio**. Están dirigidos a un usuario o al propio sistema de correo. En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo o cualquier variante, que tenga el objetivo final de paralizar el servicio por saturación de las líneas, de la capacidad de CPU del servidor, o del espacio en disco del servidor o del usuario. En inglés estos ataques se conocen como "*mail bombing*", y son un caso particular de DoS (Denial of Service, denegación del servicio). El *spam* también puede ocasionar casos de denegación de servicio por saturación y sobrecarga de los recursos de los proveedores de servicio, sin embargo su finalidad última no es imposibilitar o dificultar el servicio.

1.3. Los comienzos del spam y origen del término.

El primer *e-mail* comercial no solicitado, fue enviado de forma masiva a todos los usuarios de Arpanet en mayo de 1978 por Gary Thuerk, responsable de ventas de la empresa Digital Equipment Corp (DEC). Él pensó que los usuarios de Arpanet podrían estar interesados en conocer que DEC (empresa de informática) había integrado el protocolo que soportaba Arpanet directamente en un nuevo DEC-20, con su sistema operativo TOPS-20[132].

El protocolo SMTP que regula todas las transacciones de correo electrónico de Internet, se creó en 1981 de forma insegura para ser usado por científicos, sin pensar en ningún uso comercial. En esta época ya existían listas de distribución (como LISTSERV-1984) que eran usadas para distribuir información de uno a muchos. La explosión de Internet en 1994 a nivel social y comercial, hizo que se descubrieran los agujeros de SMTP para ser utilizado como el mejor y más barato mecanismo para distribuir y hacer llegar directamente a miles de buzones cualquier tipo de información comercial.

La generalización del uso del *spam* empezó en 1995-1996, donde cualquier máquina con un servidor de correo podía ser usada por los indeseables *spammers* para distribuir su información. El gran problema eran los ataques que sufría el puerto SMTP (25) para distribuir *spam*. En dicha época el servidor de correo más extendido era Sendmail, el cual solucionó las deficiencias de SMTP con sus reglas de configuración, con lo que se empezaron a solucionar muchos de los problemas relacionados con el protocolo. En esos años el *spam* que se recibía en los buzones era de dimensiones muy inferiores a las actuales.

Aún así, hoy en día estos problemas de configuración no están erradicados en el 100% de las máquinas de Internet, por lo que siguen existiendo servidores *open-relay*

[132] Datos obtenidos del estudio "Spam E-mail and Its Impact on IT Spending and Productivity" (diciembre de 2003), Spira, J. B., realizado por Basex Inc., www.basex.com.

(máquinas *open-relay* son servidores de correo electrónico mal configurados que permiten encaminar correo desde cualquier dirección IP). Esto permite un uso indebido de recursos de la empresa por parte de personas ajena a la misma. Estas estafetas son las preferidas por los *spammers* para inyectar mensajes de *spam* destinados a miles o millones de usuarios.

Posible origen del término spam.

Spam es una palabra inglesa cuyo origen está en una empresa charcutera norteamericana (Hormel Foods), que en 1937 lanzó una carne en lata originalmente llamada Hormel's Spiced Ham. El gran éxito de este producto lo convirtió con el tiempo en una marca genérica, es decir, que se acabó llamando al citado producto con el nombre de la compañía, igual que en España por ejemplo a Colgate, con su dentífrico. Esto ocasionó que los fabricantes le cambiaran el nombre para reducirlo, dejándolo con un nombre de cuatro letras (SPAM[133]). El SPAM fue un producto tan conocido como que alimentó a los soldados rusos y británicos en la II Guerra Mundial, y fue comercializado en todo el mundo en 1957, haciéndose aún más popular en los años 60.

La asociación de SPAM con el correo electrónico no solicitado, tiene dos versiones:

1. A raíz de una secuencia de la serie de humor por excelencia en el Reino Unido, "Monty Python", en la que se hacía una burla sobre la carne en lata. Su divertidísima costumbre de gritar la palabra SPAM en diversos tonos y volúmenes se trasladó metafóricamente al correo electrónico no solicitado, pues en los episodios de Monty Python, los gritos de la palabra *spam* perturbaban las conversaciones normales, igual que el correo electrónico no solicitado perturba las comunicaciones vía *e-mail* en Internet.
2. La otra versión es que la asociación de SPAM con el correo electrónico no solicitado, proviene de un laboratorio informático de la Universidad de California del Sur, que lo bautizó así porque presenta similitudes en sentido figurado con la carne enlatada con dicho nombre: aparece en cualquier lugar y nadie la pide en ningún caso, nadie se la come (es lo primero que se echa a un lado cuando se toman entremeses); y a veces tiene algo de sabor, como ese 0,0001% del correo electrónico no deseado que resulta útil a alguien.

La primera constancia de uso de este término se remonta a 1994, cuando dos abogados (Canter y Stegel)[134] enviaron un mensaje anunciando sus servicios a todas las listas de distribución de USENET, y los usuarios le llamaron *spam*. De cualquier manera, *spam* es una palabra comúnmente aceptada para designar al correo electrónico no deseado.

[133] Los dueños de la marca Hormel Foods, en Minessota, no registraron la palabra *spam* como marca, por lo que a efectos legales no pueden denunciar su uso para designar a cualquier otra cosa que no sea su producto. Por ello, en su página web ruegan al público que cuando se refieran a su producto de carne enlatada lo hagan con mayúsculas (SPAM), para distinguirla del correo electrónico basura, *spam*. Este es el motivo por el que en solidaridad con Hormel Foods, hemos incluido la palabra SPAM con mayúsculas, para referirnos a la carne enlatada y con minúsculas para referirnos al correo electrónico no deseado.

[134] Datos obtenidos de "Spam E-mail and Its Impact on IT Spending and Productivity" (diciembre de 2003), Spira, J. B., realizado por Basex Inc., www.basex.com.

1.4. Efectos del spam. Por qué es perjudicial.

El gran volumen de mensajes.

La facilidad y bajo coste del envío de miles de mensajes en periodos cortos de tiempo, han provocado una gran proliferación de esta práctica, que representa hoy en día más de la mitad del tráfico total que circula en Internet[135]. Esta gigantesca cantidad de mensajes, provoca en muchos casos la imposibilidad o dificultad del servicio del correo electrónico y la reducción de su efectividad por varias causas:

- El *spam* consume recursos de la estafeta de correo electrónico, ralentizando el procesamiento del correo normal.
- Afecta al ancho de banda, congestionando las infraestructuras de comunicaciones.
- Ocasiona la inundación de los buzones de los usuarios, haciendo que se rebase la capacidad máxima de los mismos y por tanto provocando la pérdida de correo deseado y útil.
- Induce al receptor a una pérdida de confianza en el correo electrónico, por la naturaleza molesta y ofensiva de muchos mensajes.

El robo de recursos a los operadores.

Los *spammer* utilizan diversas técnicas para conseguir enviar miles de mensajes de correo electrónico, de tal forma que el gasto ocasionado y la responsabilidad recaigan sobre otras personas. Nos referimos a los operadores de encaminamiento, que son los encargados del transporte del mensaje de correo entre el emisor y el receptor, y al operador de destino, que es responsable de mantener el control de los buzones de los receptores[136].

A continuación, explicamos las técnicas más usadas por los *spammers* para hacer que los costes de sus envíos masivos recaigan sobre otras personas, y por qué representan un robo de recursos:

1) La mayor parte del *spam* se envía a través de sistemas intermediarios inocentes, sin ninguna relación con el *spammer*. Así, utilizan servidores de terceros sin que éstos sean conscientes, aprovechando la peculiaridad que presentan la mayor parte de los sistemas de correo de Internet de transportar y entregar mensajes a cualquier usuario, no sólo a los propios. Esta característica hace que las redes y los dispositivos de almacenamiento de estos intermediarios se saturen de *spam* con *e-mails* que no se deberían entregar. Además provocan las quejas de los receptores, que a menudo suponen que su proveedor de correo está aliado con el *spammer*, porque le entregó el mensaje[137].
2) Otra técnica usada por los *spammers*, que también representa un robo de recursos, es la de conseguir una cuenta de acceso a Internet gratuita y hacer los envíos masivos desde ésta. Si el PSI no detecta antes al *spammer* y le cancela la cuenta, éste envía decenas de miles de mensajes y después la abandona, dejando todas las responsabilidades al PSI.
3) También es una práctica frecuente utilizar como remitente una cuenta existente o una dirección falsificada de un usuario, empresa u organización. Sobre éste recaen

[135] Consultar el apartado 2.1.3., "Cantidad de *spam* que circula en Internet".

[136] Según la organización RedIris, en su artículo "Abuso en el Correo Electrónico", se expresa que igualmente representa un abuso del correo electrónico el hecho simplemente de usar estafetas ajenas y no públicas sin su consentimiento para reenviar correo propio, aunque éste sea legítimo.

[137] Consultar el apartado 2.3.2., "El problema e implicaciones de los servidores abiertos."

las consecuencias del envío masivo de correo electrónico: desbordamiento de su buzón con los miles de *e-mails* devueltos de las direcciones que no existían, gran cantidad de usuarios que responden quejándose, etc. Se trata de un ataque muy dañino, que acarrea en muchas ocasiones tener que cambiar las cuentas afectadas.

Todo esto ha traído grandes consecuencias a los operadores. La primera un gran aumento en los costes, ocasionado por la necesidad de disponer de mayor cantidad de recursos. También por tener que disponer de mano de obra adicional para solucionar los desastres acarreados por el *spammer,* y para vigilar las actividades que se llevan a cabo desde las cuentas de los usuarios, con el fin de impedir los abusos. Por otra parte, si el *spammer* usa la segunda o tercera opción explicada, es muy probable que el operador sea incluido en listas negras[138]. Esto ocasiona además de los daños en imagen y los derivados de las denuncias de los afectados, que sus clientes son inocentes sufran las consecuencias, dejando de recibir correo electrónico durante algunos días.

Un coste social y monetario también recae en el receptor.

En efecto, si suponemos que un usuario típico dedica unos 10 segundos en identificar y descartar un mensaje, basta multiplicar este tiempo y el coste del mismo por los millones de mensajes *spam* que diariamente se transmiten en la red, para hacernos una idea de su repercusión. El tiempo de conexión que dedican diariamente los clientes de un gran proveedor a descartar los envíos no solicitados y el precio que esto supone es enorme, y esto lo pagamos todos los usuarios de Internet traducido en un mayor coste de las telecomunicaciones y los servicios. En cambio, el *spammer* puede realizar millones de envíos con inversiones bajísimas[139].

En conclusión, por una parte alguien nos hace pagar por algo que no queremos hacer ni recibir, y por otra, ninguna publicidad resulta tan barata para el anunciante y tan cara para el receptor. Para entender esto proponemos una analogía de publicidad fuera del ámbito de Internet: hacer llamadas telefónicas para promocionar un producto o servicio a cobro revertido. Todos podemos hacernos una idea de cuánto abuso representa.

Se trata principalmente de la promoción de productos o servicios fraudulentos.

El *spam* anuncia en la mayoría de las ocasiones productos y servicios que no interesan lo más mínimo al destinatario o que son engañosos y fraudulentos[140], como por ejemplo, métodos para curas milagrosas, componentes de ordenador "piratas", montajes para enriquecerse rápidamente muy vagamente descritos, o anuncios de pornografía. Así, según un análisis de la Comisión Federal del Comercio de Estados Unidos[141], de una muestra al azar de 1.000 mensajes *spam* escogidos entre 11 millones, el 66% fue considerado fraudulento. De los mensajes que ofrecían oportunidades de negocio o inversiónes tales como trabajo desde casa, fue considerado fraudulento el 96%.

[138] El tema de las listas negras será tratado en el apartado 4.1.2. ("Métodos basados en listas negras").

[139] Consultar el apartado 2.1.6., "Las cifras del negocio de los spammers", para más información al respecto.

[140] Más adelante, en el apartado 1.5., "Ejemplos de estafas, prácticas fraudulentas y engañosas que realizan los spammers", se puede comprobar dicha afirmación mediante una serie de ejemplos reales.

[141] Según Eileen Harrington, director asociado de la FTC. Datos obtenidos del artículo "Dos tercios del '*spam*' que recibimos son fraudulentos", www.iblnews.com.

Casi todos son productos inútiles que no merecen la pena o que son ilegales, ya sea por su naturaleza, o porque es ilegal promocionarlo en medios comunes en los que hay que pagar un precio por el coste del anuncio, pues están sujetos a una legislación[142].

Es ilegal.

Tanto el método usado para recopilar las direcciones de correo electrónico víctimas, como el propio hecho del envío masivo de mensajes, son combatidos por la mayoría de países y colectivos que trabajan en la red. En algunos países como en España, es ilegal desde la entrada en vigor de la LSSICE, además de que en la mayoría de las ocasiones, la dirección de correo electrónico se considera como dato personal según la LOPD[143], por lo que se estaría incurriendo en una violación de la intimidad.

El spam en los grupos de noticias y listas de distribución.

Los mensajes que se difunden a través de los grupos de noticias y listas de distribución con contenido comercial y ajeno a la temática del grupo en el que aparecen, también son *spam*[144]. Algunos intentan quitar importancia al asunto diciendo que no son *spam* sino mensajes *off topic*, es decir, que no son ilegales sino simplemente no se corresponden con el tema del grupo de distribución al que han sido enviados por algún error. Pero la diferencia entre un mensaje *off topic* y un mensaje *spam* es clara: el *spam* además de *off topic*, es comercial. Del mismo modo que los mensajes *spam* que llegan al buzón personal de correo electrónico del usuario, hacen gastar tiempo y atención, y no han sido solicitados por parte de los receptores del grupo, ya que se encuentran fuera de la temática de interés.

Estos mensajes por tanto son *spam*, y representan una lacra para estos sistemas porque aunque son no requeridos por el grupo de noticias, el usuario debe descargarlos. La única alternativa sería conectarse, bajar primero las cabeceras, limpiar los mensajes que sean *spam* y después volverse a conectar para bajarse los mensajes seleccionados, pero acarrea más coste en tiempo y dinero que resignarse a descargarse todos los mensajes.

Por otro lado consumen recursos de los servidores, lo que repercute en demoras en los tiempos de conexión, y en general, en una pérdida de eficacia y utilidad de las propias listas y grupos de noticias, además de los trastornos económicos.

1.5. Ejemplos de estafas, prácticas fraudulentas y engañosas que realizan los spammers.

Cuando hemos comentados los distintos abusos del correo electrónico y los efectos del *spam* en esta introducción, hemos citado las consecuencias perjudiciales que se derivan de su uso y los métodos fraudulentos que se utilizan para que el coste de los envíos recaiga en otras personas. Todas las técnicas comentadas son ejemplos de estafas que realizan los *spammers*[145].

[142] Consultar el apartado 3.1. del bloque II, en el que se indican unos breves apuntes sobre la legislación que rige la publicidad.

[143] Consultar el apartado 3.1. del bloque II de este trabajo en el que se analizaban las consecuencias legales de este tema.

[144] Según la definición de *spam* que hemos realizado en el apartado 1.2. ("Definición del *spam*"), sería *spam* en cuanto a que se trata de un envío masivo no solicitado (a toda la lista), y en cuanto a que es comercial.

[145] Consultar el apartado 1.4., "Efectos del *spam*. Por qué es perjudicial".

Por otra parte las estafas, fraudes y engaños que llevan a cabo los *spammers,* pueden ser derivados del contenido de los mensajes, con lo que se realizan al receptor, no al operador. El engaño puede llevarse a cabo mediante los campos de la cabecera, o mediante el cuerpo del mensaje.

Los campos de los que consta la cabecera del mensaje, en la mayoría de las ocasiones son falsos. En efecto, según las conclusiones de un estudio realizado por la Comisión Federal del Comercio de Estados Unidos (FTC)[146], el 33% del *spam* analizado contiene información falsa en el campo "*From*:" ("De:") y el 22% de los mensajes contienen información falsa en el campo "Subject:" ("Asunto:"). La mayoría de ellos sugieren una relación con el receptor del mensaje, para aportar credibilidad.

Así, el *spam* es un canal ideal para llegar a un público desprotegido al que es más fácil de timar, como pueden ser niños, personas mayores o cualquier usuario confiado. Aquí se han recopilado algunos de los engaños más comunes que se llevan a cabo en el contenido del mensaje, que según la FTC contiene signos de falsedad en el 40% de los casos.

- Cartas en cadena y hoaxes. Las cartas en cadena que incluyen dinero, artículos valiosos y prometen grandes beneficios son una estafa. Así, los usuarios que empiezan una de estas cadenas o contribuyen a propagarla enviándola a alguien, están contribuyendo a ese engaño. Los hoaxes también son un tipo de fraude, que persigue ante todo conseguir direcciones de correo electrónico para enviar *spam*[147].
- Trabajos desde casa. Los mensajes con ofertas para trabajar desde casa, a menudo son un fraude e incumplen sus promesas, pues al final el usuario trabaja muchas horas, asume costes de papel, fotocopias, y cualquier otro material necesario para el trabajo, sin recibir nada a cambio. O a veces el beneficio recibido no compensa los costes. En otras ocasiones, las compañías que encargan estos trabajos solicitan que se abone una cantidad para recibir las instrucciones o los programas tutoriales que nunca llegarán, y de aquí sacan su beneficio.
- Métodos para perder peso. Nos referimos con ello a los programas y productos que promueven la pérdida de peso de manera rápida y sin esfuerzo. Todos los testimonios y garantías que se dan en el mensaje no tienen ningún valor, por lo que nunca se debe hacer caso de lo que digan. Además, concretamente estos temas, deben siempre ser tratados por un médico.
- Créditos o préstamos. Se debe ser cauto con los *e-mails* que ofrezcan servicios financieros por entidades no conocidas, pues prometen facilidad para concederlos sin consultar la situación financiera en la que nos hallamos. Puede ser una manera encubierta de conseguir el número de cuenta, por ejemplo y estafar al usuario.
- Contenidos para adultos. Los mensajes que ofrecen contenidos para adultos gratuitos, pueden hacer que se instale un programa que desconecte la conexión a Internet del usuario, y en su lugar redireccionar la conexión a algún número de tarificación adicional o con prefijo internacional con precio mucho más alto y que destine parte de éste al beneficio del estafador.
- Basados en la realización de llamadas. Estos anuncios ofrecen falsas participaciones en concursos, superofertas o servicios que requieren de una llamada o enviar un fax a un número de los servicios de tarificación adicional a través de los 803, 806 y 807, (que antes se gestionaban a través de los 906 y 903), o con prefijo internacional.

[146] "False Claims in Spam, a report by the FTC's Division of Marketing Practices", abril de 2003. Federal Trade Commission. Para más información sobre el tema, consultar el apartado 2.4. de este trabajo, "Análisis de las cabeceras de los mensajes."

[147] Consultar el apartado 2.2.2., "Un método que conlleva además otros graves daños: el hoax".

- Promoción de la técnica de *spam*. Utilizar el *spam* para convencer a empresas de que el *spam* es una receta mágica y barata para hacer crecer y dar a conocer los negocios de aquéllos que contraten sus servicios. Por ejemplo, una empresa fraudulenta de marketing, promete a un cliente que enviará mensajes a gente que ha solicitado recibir información sobre nuevos productos y servicios. Sin embargo, lo que la empresa que contrata los servicios del *spammer* a menudo consigue, es crearse enemigos que nunca comprarán nada tras haber recibido estos mensajes no solicitados, e incluso perder algunos de sus clientes.
- Para intentar que los receptores no consideren su mensaje como *spam* y conseguir que el usuario lea el mensaje con cierta confianza de su veracidad, a veces crean falsos sitios *web antispam*, o falsifican los mensajes electrónicos como procedentes de organizaciones que luchan contra el *spam*.
  Además, normalmente adjuntan algún modo en que el usuario puede pedir que su dirección no vuelva a ser utilizada para enviar *spam*. Sin embargo, casi nunca es cierto[148]. En otras ocasiones facilitan un número de teléfono de otro continente al que se debe llamar. El precio de la llamada desanima a los usuarios.

En definitiva, el *spam* representa un canal barato para incurrir en todo tipo de timos, estafas y prácticas fraudulentas e ilegales, que aunque podrían castigarse mediante el código penal o por la ley de publicidad engañosa, a menudo son difícilmente perseguibles. Además, estos mensajes pueden incluir algún dispositivo de rastreo (como el *web bug*[149]), con lo que al abrir el mensaje automáticamente se está informando al *spammer* de que la dirección del receptor está activa, y con ello nos predisponemos a recibir todo tipo de publicidad y *spam*.

[148] El estudio "Remove Me Surf", realizado por la Federal Trade Comisión de EEUU, encontró que 63% de las listas de *e-mail* no eran honestas con las peticiones de los usuarios de borrar su dirección de la lista de envíos de *spam*.

[149] Consultar el apartado 3.2. del bloque II, "Obtención de datos ilícitos con fines de marketing".

2. Análisis.

2.1. Análisis de la situación del spam en cifras. Estudios y estadísticas.

2.1.1. Introducción.

En este apartado se han analizado y comparado los resultados de diferentes estudios sobre el *spam*, con el fin de aportar una serie de datos más o menos objetivos acerca de qué tipos de negocios se promocionan mediante *spam*, qué volumen de *spam* circula en Internet, cuáles son los costes que ocasiona y la opinión de los usuarios. Por último también se han incluido unos datos interesantes obtenidos de unas entrevistas realizadas a varios *spammers*, que pueden aportarnos cómo ven ellos el *spam* desde su punto de vista.

2.1.2. Naturaleza del *spam*.

2.1.2.1. Categorías.

El tipo de productos y servicios que se intentan promocionar a través del *spam* son básicamente productos financieros, bienes de consumo y pornografía. Para realizar el siguiente análisis se han tenido en cuenta los resultados de tres estudios[150]: de la Asociación de Usuarios de Internet en España (AUI), de la Comisión Federal del Comercio de Estados Unidos (FTC) y de la compañía norteamericana Clearswift, cuyos resultados se muestran en la siguiente tabla.

[150] El estudio realizado por la AUI se llevó a cabo durante el mes de abril de 2003, en el que se recibió un total de 5.627 mensajes no solicitados recibidos en sus cuentas de correo electrónico. El estudio de la Comisión Federal del Comercio de Estados Unidos de Estados Unidos, "False Claims in Spam, a report by the FTC's Division of Marketing Practices", fue realizado en abril de 2003 analizando 1000 mensajes *spam* tomados de una muestra aleatoria de más de 11 millones de mensajes *spam*. Por último, el estudio "Índice de Spam" realizado por la compañía norteamericana Clearswift en su tercera edición (junio-agosto 2003) fue realizado para explicar las tendencias y usos del marketing directo a través de Internet. Los resultados de este estudio han sido tomados del artículo "Los productos de consumo y de salud son los que más utilizan el Spam", www.noticiasdot.com.

Tabla 11. Comparativa de los productos y servicios promocionados mediante spam.

Fuentes: FTC, AUI, y estudio Clearswift.

AUI	FTC	Clearswift
		Bienes de consumo (31%)
Vacaciones (12%)	Viajes / Ocio (2%)	
Informática / Internet (software + ordenadores y periféricos) (10%)	Informática / Internet (7%)	
	Otros productos / servicios (16%)	
-	Educación (1%)	-
-	Salud (10%)	Salud (21,2%)
Pornografía (15%)	Contenidos de adultos (18%)	Pornografía (13,6 %)
Productos financieros (12%)	Productos financieros (17%)	Productos financieros (17,2%)
Trabajo fácil (10%)	Inversiones / Oportunidades de negocio (20%)	-
	Otros (9%)	Otros (5,4%)
Casinos / juegos de azar (14%)	-	Ofertas de juegos (6%)
Sorteos (11%)	-	
Cartas encadenadas (7%)	-	-
-	-	Estafas y timos 2%
-	-	Spam interrelacionado 3,6%

Dado que los estudios estaban planteados desde diferentes perspectivas, para poder establecer una comparación entre ellos se han distribuido los temas de manera que los que se refieran a grupos similares queden colocados en la misma fila de la tabla. Así en el estudio de Clearswift, se observa que los bienes de consumo representan el tema con mayor porcentaje de *spam* observado, que podrían compararse con el porcentaje de *spam* relacionado con ocio y vacaciones, así como con productos relacionados con la informática e Internet. Los temas que se presentan en los tres estudios con porcentajes similares son los contenidos pornográficos y los productos financieros, por lo que no cabe lugar a dudas que se trata de dos grupos muy presentes en el *spam*. Por otro lado, se observa que en Estados Unidos (estudios de la FTC y de Clearswift) aproximadamente un 20% del *spam* está relacionado con temas de salud. En el estudio realizado a usuarios españoles (AUI), es importante el porcentaje referido a sorteos, casinos y juegos de azar (un 35%).

2.1.2.2. Días, horas y tamaños de los mensajes.

Durante el mes de abril de 2003, la AUI recolectó los mensajes no solicitados recibidos en sus cuentas de correo electrónico con el fin de elaborar estadísticas por hora, día, mes, y su evolución en cantidad y tamaño. De este estudio realizado con un total de 5627 *e-mails* no solicitados que se recibieron, a razón de 201 por día, se extrajeron las siguientes conclusiones:

- Lunes y martes parecen ser los días preferidos por los *spammers* para enviar sus mensajes, decayendo hacia el fin de semana. Jueves y domingos aparecen como los días menos propensos para realizar esta actividad.
- El horario preferido por los *spammers* es desde las 13:00 a las 18:00 horas, mientras que el más desfavorable parece ser la madrugada. Si tomamos en cuenta que el 80% estaba escrito en inglés, podríamos deducir que este horario coincide con las primeras horas de actividad en Estados Unidos (de 8 de la mañana a la 1 del medio día).

- En cuanto al tamaño, la inmensa mayoría de los *spammers* envía mensajes inferiores a 10 *Kilobytes*, aunque se recibieron casi 30 mensajes no solicitados superiores a 40 *Kilobytes*.
- En total, recibieron unos 32,8 *Megabytes* de *spam*, un promedio de casi 1,2 *Megabytes* por día, lo cual para un usuario de Hotmail (cuyo buzón tiene una capacidad de 3 *Megabytes*) por ejemplo, significaría el bloqueo de su cuenta en menos de dos días.

Se advierte una evolución importante en la cantidad de *spam* recibido desde los primeros días hasta finales del mes de estudio, lo que indica la tendencia creciente del *spam*, aunque el periodo de estudio sea de solamente un mes.

2.1.2.3. Origen del *spam* por países.

Un estudio realizado durante el mes de marzo de 2003 por la compañía MessageLabs, proveedora de sistemas de seguridad informática, analizó el origen de 104 millones de mensajes *spam*. Este estudio indica los porcentajes de mensajes clasificados por país de origen. A continuación se adjunta un gráfico en el que pueden observarse.

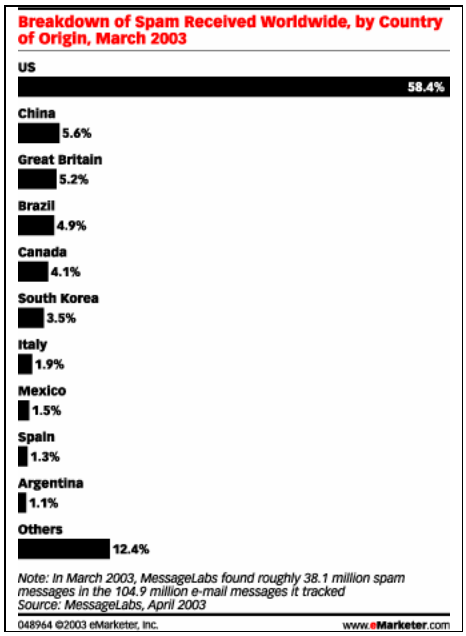

Ilustración 37. Países emisores de spam. Fuente: Fuente: www.vanderreis.com[151]

El primer país "productor" de *spam* es Estados Unidos con el 58% de los mensajes, seguido muy de lejos por otros países como China (5,6%), Gran Bretaña (5,2%), y Canadá (4,1%). Estas cifras corroboran el hecho comprobado por todos de que la mayoría del *spam* está escrito en inglés. Otro dato interesante es que España está

[151] Esta gráfica ha sido obtenida de la página www.vanderreis.com, publicada con permiso de Emarketer.com. La compañía que realizó el estudio fue MessageLabs, en marzo de 2003.

entre los 10 primeros países productores de *spam*, aún contando con una ley que lo prohíbe[152].

2.1.3. Cantidad de *spam* que circula en Internet.

Según los datos que baraja el Ejecutivo comunitario[153], en 1999 el porcentaje de tráfico debido a los mensajes *spam* frente al total del tráfico en Internet era del 5%, en 2001 representaba el 7% del total, y en 2003 representa más de la mitad del tráfico de Internet, de modo que el tráfico debido al *spam* se ha multiplicado por siete en tan solo dos años, por lo que se ha convertido en una amenaza para el desarrollo y la confianza de los usuarios en las comunicaciones electrónicas. En la siguiente gráfica podemos apreciar esta tendencia de crecimiento exponencial.

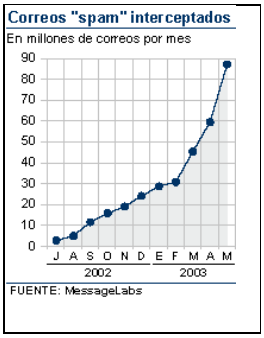

Ilustración 38. Tendencia del volumen de *spam*.

Fuente: www.elmundo.es/navegante.

Sin embargo estas cifras no muestran el volumen de *spam* en Internet en la segunda mitad del año 2003 y principios de 2004. Para ver qué ha ocurrido en el último año, podemos ver los datos aportados por el estudio realizado por Brightmail[154]. Éste indica que el *spam* representó en febrero de 2004 el 62% de los *e-mails* que se envían y reciben en Internet. Según esta compañía el número de mensajes que circuló en 2003 fue de $12{,}5*10^{12}$, lo cual representaría un número de mensajes *spam* de $7{,}75*10^{12}$ para 2004[155]. En la gráfica siguiente puede apreciarse la tendencia del porcentaje de *spam* en Internet desde marzo de 2003.

[152] Consultar los apartados 3.1.1. del bloque II, "Legislación en torno a la comunicación o promoción *on line*", y 3.3.1.1. de este bloque, "Situación en España".

[153] Esta información ha sido obtenida del artículo "La UE anuncia medidas contra el '*spam*' por la desconfianza que causa" (27 de enero de 2004), www.elmundo.es/navegante.

[154] Esta información ha sido obtenida del sitio web www.aui.es/contraelspam.

[155] Esta cifra se ha calculado suponiendo que el crecimiento del *spam* se estancara en el 62% para 2004 y que el número de mensajes en este año fuera igual que en 2003. Estas suposiciones apuntan que la previsión es bastante conservadora.

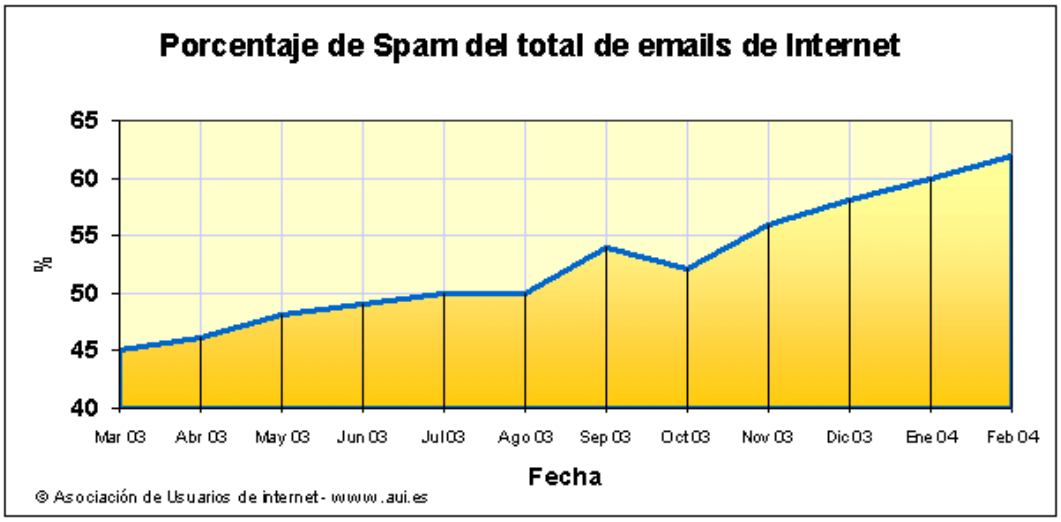

Ilustración 39. Tendencia del volumen de *spam*.

Fuente: Brightmail, www.aui.es/contraelspam.

En la gráfica se aprecia un pico significativo del volumen de *spam* entre agosto y octubre de 2003. El máximo entre estas fechas tuvo lugar concretamente el 26 de agosto de 2003 y fue debido al efecto del virus Sobig, el cual batió todas las marcas de *spam*. Un aspecto a destacar, es que los datos presentados para mediados de 2003 hablaban de que el *spam* representaba aproximadamente el 50% del tráfico de Internet a fecha de julio de 2003. Sin embargo después de la infección del virus, los niveles de *spam* no volvieron a niveles de fechas anteriores, sino que tras la desinfección de los equipos, el *spam* continuó creciendo con una tendencia al alza aún más acusada. Visto esto, podemos pensar que la este crecimiento aún puede aumentar más y más, dado que otros virus más recientes como el MyDoom, se han extendido por Internet con la misma filosofía.

2.1.3.1. Cantidad de *spam* recibido por los internautas.

Para analizar el número de mensajes *spam* recibidos por los internautas españoles hemos analizado varios estudios. En primer lugar presentamos los resultados de las encuestas realizados por la AIMC en 2001 y 2002, que representan el usuario medio español de correo electrónico con una edad superior a 14 años[156].

[156] "4ª encuesta a Usuarios de Internet de la AIMC febrero 2001" y "5ª encuesta a Usuarios de Internet de la AIMC febrero 2002". Las encuestas se realizaron a una base imponible de 43.592 usuarios que poseen *e-mail*. Fue realizada en febrero de 2001 (4ª Encuesta) y en febrero de 2002 (5ª Encuesta) a una muestra del EGM que es probabilística y representativa de la población española de 14 ó más años.

Tabla 12. Número de mensajes *spam* que reciben los usuarios. Fuente: AIMC, 2001 y 2002.

¿Con qué frecuencia recibe mensajes no solicitados/deseados?	AIMC F-2001	AIMC F-2002
Más de uno al día	17,8 %	40,3 %
Uno al día	4,4 %	4,9 %
Varios a la semana	25,1 %	27,3 %
Uno a la semana	5,4 %	3,5 %
Varios al mes	13,2 %	9,3 %
Uno al mes	4,9 %	2,5 %
Con una frecuencia menor	14,9 %	7,6 %
Nunca he recibido ninguno	14,1 %	4,3 %
NS/NC	0,3 %	0,3 %

Lo más destacable de los resultados mostrados, es que un 22,2% de los usuarios de correo electrónico padecía el *spam* en 2001 y casi la mitad (un 45%) en 2002. Además observamos cómo decrece el porcentaje de usuarios que reciben *spam* con frecuencias menores de varios por semana. Son datos importantes a tener en cuenta porque se refieren a un usuario español medio mayor de 14 años, no a usuarios experimentados que hacen gran uso del servicio.

A continuación adjuntamos los gráficos obtenidos de un estudio realizado por la AUI entre abril y mayo de 2003[157].

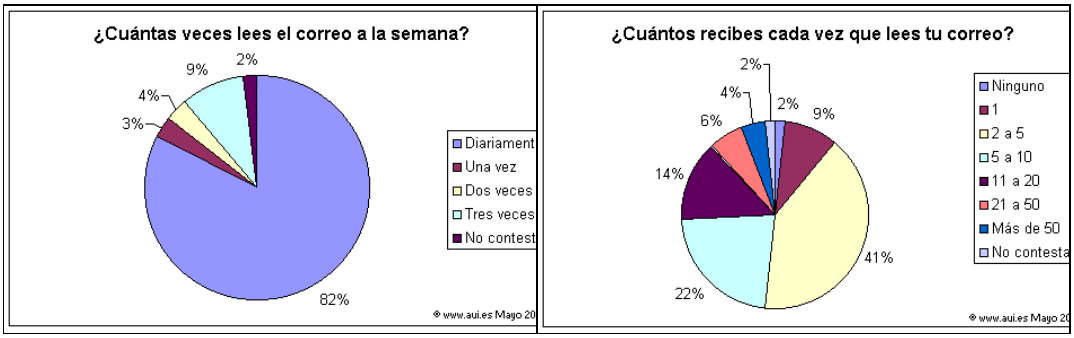

Ilustración 40. Frecuencia de lectura y número de mensajes *spam* recibidos por los usuarios. Fuente: AUI, 2003.

El gráfico de la derecha, muestra los porcentajes de usuarios que reciben el número de mensajes *spam* indicados. Se observa que la mayoría de los usuarios recibe entre 2 y 5 *e-mails* no solicitados (un 41%). Es significativa también la proporción de usuarios que reciben más de 20 (un 10%), destacándose un 4% que recibe más de 50 mensajes *spam* cada vez que lee su correo, suponiendo que se lee el correo el número de veces a la semana indicado en el gráfico de la izquierda (82% a diario).

[157] Encuesta realizada por la Asociación de Usuarios de Internet (AUI) a través de su página web (www.aui.es) entre abril y mayo de 2003, con un número de respuestas de 2054. Hay que tener en cuenta que esta encuesta no es representativa de la población total española, al igual que la efectuada por la AIMC, sino de un porcentaje de internautas experimentados y con interés sobre el tema, que navegan en la página de esta asociación y que están lo suficientemente concienciados con el tema para rellenar la encuesta, lo que indica que están claramente en contra del *spam*.

Estos resultados muestran que el *spam* no es sólo un problema que afecta a las empresas, o a las cuentas de usuarios avanzados y administradores, cuyas cifras exponíamos en el apartado anterior, sino que afecta a todos los usuarios. Así, los datos nos indican que en Hotmail, el proveedor de correo *web* más utilizado de Internet con 110 millones de usuarios, transcurridos varios días de abrir una cuenta de correo (aunque no se haya usado), el internauta podrá comprobar cómo el 80% de los mensajes que recibe son *spam*[158]. Algo parecido ocurre con otros grandes proveedores, como American Online, que indicó[159] que bloquea unos 2.000 millones de mensajes de correo masivo a diario, una media de 67 por cada cuenta de *e-mail*.

Este gran volumen de mensajes recibidos por los internautas, redunda en un coste y en el empleo de tiempo en borrar y clasificar los mensajes no deseados. Así, según Basex[160], los usuarios gastan unos 15 minutos diarios en comprobar y borrar el *spam* que les llega.

2.1.4. Costes derivados del *spam*.

2.1.4.1. Costes que afrontan las empresas.

El instituto estadounidense especializado Basex, realizó un estudio en diciembre de 2003[161] para intentar estimar los costes que supone el *spam* a las compañías en el mundo. Para ello estimó que los gastos de las empresas debidos al *spam*, pueden clasificarse en:

- pérdida de productividad de los empleados,
- saturación de los sistemas de correo electrónico,
- ancho de banda,
- costes de almacenaje,
- soporte a los usuarios,
- software *antispam*,
- formación a los usuarios.

Con todo ello estimó un gasto de cerca de 20.000 millones de dólares al año en todo el mundo. Tal y como afirma el estudio, las pérdidas oscilan entre los 600 y los 1.000 dólares por salario y empleado al año, lo que implica que, por ejemplo, una empresa con 15.000 trabajadores contratados afronta un gasto anual de más de 12 millones de dólares sólo por culpa del *spam*.

Otro estudio anterior publicado por el Instituto Ferris Research[162] en enero de 2003, estimaba que el *spam* iba a costar unos 10.000 millones de dólares en 2003 tan solo en las empresas estadounidenses. Durante el 2002, para las mismas empresas, el

[158] Datos obtenidos del artículo "¡Muerte al *spam*!" (30 de abril 2003), Rodríguez, G., www.libertaddigital.com.

[159] "El volumen del correo masivo amenaza el futuro del '*e-mail*'" (1 de mayo de 2003), www.iblnews.com.

[160] Dato obtenido del estudio "Spam E-mail and Its Impact on IT Spending and Productivity" (diciembre de 2003), Spira, J. B., realizado por Basex Inc., www.basex.com.

[161] "Spam E-mail and Its Impact on IT Spending and Productivity" (diciembre de 2003), Spira, J. B., realizado por Basex Inc., www.basex.com.

[162] Información obtenida de los artículos "El '*spam*' cuesta 20.000 millones de dólares a las empresas en todo el mundo" (30 de diciembre de 2003), www.elmundo.es/navegante y "¡Muerte al *spam*!" (30 de abril 2003), Rodríguez, G., www.libertaddigital.com.

coste del *spam* ascendió a 9.000 millones de dólares, mientras que para las europeas ascendió a los 2.500 millones. El cálculo realizado por la firma Ferris Research, tuvo también en cuenta la utilización de ancho de banda, el uso de soporte técnico y la pérdida de productividad del trabajador, que representaban aproximadamente un 40% sobre el total de pérdidas financieras.

Estos datos han hecho que las compañías y los gobiernos, no sólo los proveedores de servicio, se hayan tomado en serio este problema.

2.1.4.2. Costes que afrontan los usuarios.

Los usuarios también deben hacer frente a los costes derivados del *spam*. Por un lado indirectamente, puesto que si las compañías tienen que afrontar un gasto extra, esto se traducirá en algunas ocasiones en un aumento de los precios de los servicios que les presten.

De forma directa, el usuario también debe hacer frente a costes, sobre todo derivados del tiempo que necesita para limpiar su buzón de *spam*. Podemos concluir que éste no es nada despreciable, dados los datos de la cantidad de mensajes que reciben los usuarios cada vez que abren su correo, expuestos anteriormente.

2.1.5. La opinión de los usuarios.

Como se ha deducido del análisis que se está llevando a cabo, todos nos vemos afectados por el problema, aunque los afectados más directamente son las compañías, debido a los grandes costes que deben afrontar. Sin embargo, desde el punto de vista de este trabajo, lo más interesante es analizar cuál es la opinión de los internautas y cuáles son sus reacciones ante el *spam*. Para conocer estos datos hemos llevado a cabo un análisis de los resultados de varios estudios a los que haremos mención a lo largo de este apartado, entre ellos, el del centro de investigaciones Pew Internet and American Life Project[163], los de la AIMC para los años 2001 y 2002, el de la AUI[164], y el realizado por TACD[165]. Se recomienda consultar este último estudio al completo en el anexo de este trabajo, puesto que en mi opinión representa la opinión de los usuarios en todo el mundo en relación al tema. Veamos pues las conclusiones de este análisis.

[163] Estudio realizado en junio de 2003 entre 1.400 usuarios de Internet. Datos obtenidos del artículo "Los internautas esconden sus direcciones *e-mail* por miedo al "*spam*"", www.noticiasdot.com.

[164] "4ª encuesta a Usuarios de Internet de la AIMC febrero 2001" y "5ª encuesta a Usuarios de Internet de la AIMC febrero 2002". Las encuestas se realizaron a una base imponible de 43592 usuarios que poseen *e-mail*. Fue realizada en febrero de 2001 (4ª Encuesta) y en febrero de 2002 (5ª Encuesta) a una muestra del EGM que es probabilística y representativa de la población española de 14 ó más años.

La encuesta fue realizada por la Asociación de Usuarios de Internet (AUI) a través de su página web (www.aui.es) entre abril y mayo de 2003, con un número de respuestas de 2.054.

[165] "Consumer Attitudes Regarding Unsolicited Commercial Email (Spam)", octubre-diciembre de 2003. Realizado por TACD (Transatlantic Consumer Dialogue), y obtenido de http://www.tacd.org/docs/?id=225. TACD es un foro de 65 organizaciones de consumidores de la Unión Europea y Estados Unidos, que desarrolla acuerdos trasatlánticos sobre recomendaciones a los gobiernos europeos y estadounidenses en políticas comerciales. El estudio se realizó mediante una encuesta a 21.102 personas de 36 países. Se observa que los porcentajes de las respuestas de las personas de los distintos países eran similares, por lo que se concluye que la opinión sobre el *spam* es global.

2.1.5.1. Actitud de los usuarios ante el *spam*.

Como ya hemos dicho, los más afectados por el *spam* desde el punto de vista económico son las grandes compañías y los proveedores de servicio de Internet. Por ello en la mayoría de las ocasiones ellos sí tienen una visión más o menos adecuada de la dimensión del problema. Sin embargo, los usuarios no están adecuadamente informados.

Es interesante saber que a principios de 2003, el 69% de los usuarios españoles de correo electrónico no sabía qué es el *spam*, según un estudio realizado por Yahoo[166]. Este mismo indica que los usuarios españoles y los franceses son los que consultan su correo electrónico con menos frecuencia en Europa. Curiosamente, el *spam* es la primera causa de stress de los usuarios alemanes, por delante de los atascos de tráfico o de las compras navideñas.

Sin embargo durante el año 2003, el espectacular aumento del correo electrónico no deseado ha propiciado repercusiones en el concepto que los usuarios tienen del correo electrónico. En efecto, todos los estudios consultados realizados durante el año 2003, coinciden que el usuario medio del correo electrónico opina que el *spam* es muy molesto (entre un 96% y 92%). Además, según el estudio de Pew Internet and American Life Project, la mitad de todos los usuarios de Internet encuestados dice que el *spam*, les ha hecho tener menos confianza en todo el *e-mail* en general, mientras que uno de cada cuatro señala que ahora usa el correo electrónico menos, debido al *spam*. La mayoría de los encuestados dijo que no daba su dirección electrónica a los sitios *web*, en un esfuerzo por mantenerse fuera de las listas de los *spammers*. El mismo sondeo encontró que la mayoría siente que puede hacer poco para bloquear los mensajes que llegan a sus buzones electrónicos todos los días, y más de la mitad dijo que la inundación de *spam* hace difícil encontrar los mensajes que desean. Resultados similares se desprenden del estudio realizado por TACD, en el que el 52% de los usuarios ha comprado menos o nada en Internet debido a su preocupación por el *spam*.

Lo que más debería preocuparnos de los resultados de ambos estudios (ambos coinciden en este punto), es el hecho de que aproximadamente la mitad de los usuarios encuestados tiene menos confianza en Internet en general, lo que le ha llevado a comprar menos a través de este medio y a usar menos el correo electrónico.

2.1.5.2. La opinión de los usuarios acerca de las medidas que deberían tomarse para combatir el *spam*.

Al igual que hemos venido haciendo en otros apartados, comenzamos el análisis de la opinión de los usuarios acerca de las medidas que deberían tomarse para combatir el *spam* analizando los estudios de la AIMC para los años 2001, 2002 y 2004[167]. Hemos de interpretar los resultados teniendo en cuenta que a principio de los años 2001 y 2002, un porcentaje muy importante de usuarios españoles (un 69%) no conocían el problema y su trascendencia, por tanto la siguiente tabla debe entenderse desde esta perspectiva. En todo caso, observamos ya el rechazo y la preocupación por tomar alguna medida

[166] Información obtenida del artículo "Las cifras del correo basura", A. B. F., www.elmundo.es/navegante.

[167] La encuesta se realizó a una base imponible de 43.592 usuarios que poseen *e-mail*. Fue realizada en febrero de 2001 y febrero de 2002 por AIMC a una muestra del EGM que es probabilística y representativa de la población española de 14 ó más años.

para combatir el problema (72,6% en 2001 y el 83% en 2002). Veamos los resultados en la siguiente tabla.

Tabla 13. Opinión de los usuarios acerca de posibles medidas para solucionar el problema del *spam*. Fuente: AIMC, 2001 y 2002.

¿Con cuál de las siguientes respuestas está más de acuerdo en relación con el *spam*?	F-2001	F-2002	F-2004
Dada su utilidad habría que promover su desarrollo.	3,8 %	3%	1,3%
No hacer nada. La situación está bien tal como está.	8,2 %	5%	2,9%
Debería prohibirse legalmente esta práctica.	21,7 %	30%	32,4%
Crear lista de empresas/personas que realizan estas actividades para filtrar mensajes.	21,9 %	25%	25,6%
Crear registro con direcciones de aquellos que no quieran recibir mensajes (lista Robinson).	29 %	28%	30,4%
No sé, no tengo opinión al respecto.	13,5 %	8%	6,6%
NS/NC	1,9 %	1%	0,8%

Del año 2001 al 2004 se observa cómo aumenta significativamente el porcentaje de usuarios que piensan que debe prohibirse o crear listas negras, y decrecen los porcentajes de todas las demás contestaciones relacionadas con no tomar medidas, o que no se tiene opinión acerca del tema.

Datos tomados del estudio de TACD (a fecha de diciembre de 2003) y de usuarios de distintos países, muestran que el 82% de ellos piensa que los gobiernos deberían permitir que se les enviaran mensajes sólo habiéndolos solicitado previamente (*opt-in*), el 14% permitiendo el envío de mensajes siempre y cuando se facilite una forma de darse de baja de la lista (opt-out), y sólo el 2% considera que no hay que tomar ninguna medida.

La AUI en España fue más allá y preguntó a los internautas que quién debería perseguir esta práctica. Los resultados se muestran en el siguiente gráfico.

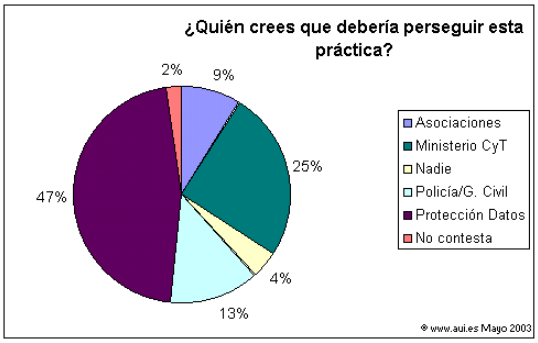

Ilustración 41. Opinión de los usuarios a cerca de qué organismo debería perseguir el *spam* en España. Fuente: AUI, 2003.

2.1.5.3. Reacción del usuario tras recibir los mensajes.

Según TACD, el 62% de los usuarios encuestados dice que usa algún tipo de filtrado como forma de combatir el *spam*, pero sólo el 17% afirma que funcionan bien.

Un dato interesante es que un elevado porcentaje de los usuarios se queja a alguien de los *e-mails* no deseados (según el estudio de Gartner Group[168], el 44% de los encuestados, de los que el 64% envían improperios al origen del *spam*, 53% se quejan al proveedor de acceso de Internet, 34% al proveedor del *spammer*, 24% a la compañía que se beneficia del *spam*, 10% a amigos y conocidos y otro 10% al Gobierno). Por otra parte, según el estudio del TACD, el 24% se queja al emisor del mensaje, el 21% a su proveedor de Internet, el 14% al proveedor del que proviene el mensaje, el 9% a alguna organización de lucha contra el *spam* y el 4% a alguna agencia gubernamental. Esta predisposición de los usuarios a efectuar una queja es muy positiva, ya que demuestra que los usuarios están comprometidos con la causa.

Sin embargo, según el estudio del centro de investigaciones Pew Internet and American Life Project, alrededor del 7% dijo que ha comprado un producto o servicio que le fue ofrecido en un *e-mail* no solicitado, mientras que un tercio indicó que había hecho *click* en un enlace para obtener más información proporcionado por un mensaje *spam*. Y por último, dos tercios de ellos dijeron que habían hecho *click* en un enlace para ser retirados de una lista de *e-mail* de *spammers*. Dados estos últimos datos, el usuario en este punto sí necesitaría tener más información, puesto que responder de alguna manera a estos mensajes es lo que propicia que el *spam* sea rentable para alguien[169].

2.1.6. Las cifras del negocio de los *spammers*.

Por último, hemos creído ilustrativo comentar algunas cifras que se barajan acerca de las ganancias de los *spammers*, la tasa de respuesta que se deriva del *spam*, etc. Hay que destacar que estas cifras no están soportadas por estudios objetivos (al igual que en apartados anteriores), sino por testimonios y supuestas entrevistas a *spammers*, por lo que se advierte que estos datos sólo deben tomarse a modo de curiosidad.

Algo a destacar es la afirmación de Steve Linford, del proyecto Spamhaus (www.spamhaus.org), con gran experiencia en la lucha contra el *spam*, que dice que 150 *spammers* son responsables del 90% del total del *spam* que circula.

En primer lugar, en el siguiente gráfico se demuestra cómo es de rentable promocionarse mediante *spam* para cierto tipo de negocios. En el gráfico se aprecia la evolución de visitas que experimentó un sitio *web* anónimo dedicado a la pornografía, tras promocionarse mediante *spam*.

[168] Los principales resultados de este estudio han sido obtenidos del artículo "La mayoría de los cibernautas son víctimas del correo indeseado", Tortello M. A., www.aui.es.

[169] Consultar el siguiente apartado, 2.1.6., "Las cifras del negocio de los *spammers*".

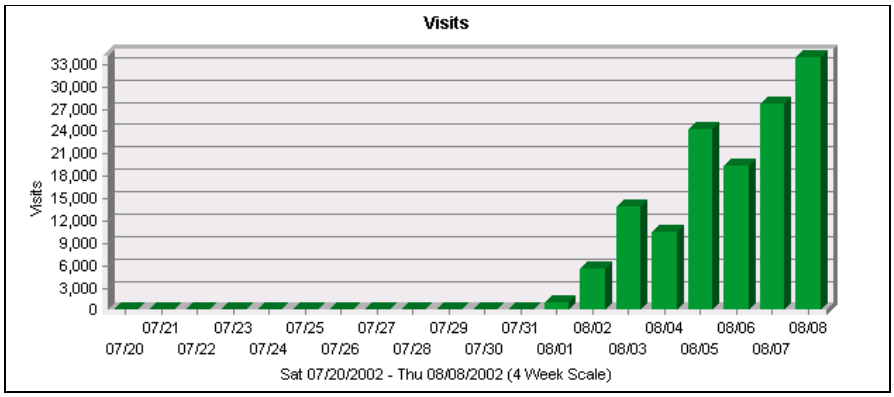

Ilustración 42. Tasa de visitas de un sitio *web* pornográfico tras promocionarse mediante *spam*. Fuente: www.xtdnet.nl/paul/*spam*/ueff[170].

Se aprecia cómo desde el 20/07/2003 que comienzan los envíos hasta el 08/08/2003 (menos de un mes) el número de visitas del sitio *web* aumenta desde un número insignificante de ellas, hasta 33.000.

Pero ¿cuánto son los honorarios de un buen *spammer*? ¿Cuáles son los recursos que deben emplear para ello? Las respuestas a estas preguntas las encontramos en un artículo[171] del "Detroit Free Press" en el que se dice haber entrevistado a uno de los mejores *spammers*, Ralsky, que con 57 años dice ser el maestro del *spam* más viejo. Vive en una casa de 740.000 dólares (en un lugar que mantiene en el anonimato para evitar las amenazas de las que es víctima por parte de *antispammers*), tras irse al extranjero para evitar las leyes contra el *spam* del estado de Virginia, donde operaba anteriormente. El *spam* le ha hecho rico, promocionando sobre todo métodos para perder peso, casinos *on line*, ofertas para vacaciones, hipotecas o farmacias *on line*. Dispone de 20 ordenadores dispuestos en array, servidores y una línea de alta velocidad (de tipo T1). Controla 190 servidores de correo electrónico, 110 localizados en el sur de Estados Unidos, 50 en Dallas, y 30 más en Canadá, China, Rusia y la India.

En 1997 comenzó su carrera como *spammer* consiguiendo 6.000 dólares en una semana por hacer un envio masivo. Hoy, según Ralsky, cada computadora es capaz de enviar sobre 650.000 mensajes cada hora (más de un billón al día), encaminados a través de empresas de Internet extranjeras deseosas de venderle ancho de banda.

Según John Mozena of Grosse Pointe Woods, fundador de Coalition Against Unsolicited Commercial E-Mail (www.cauce.org), una organización de lucha contra el *spam*, sus operaciones son sofisticadas, siendo difícil de localizar el emisor, por usar cientos de dominios para enviar su *spam*.

Dice trabajar en ésto 18 horas al día, y su modo de operación es el siguiente: por un lado, se concentra en actualizar y aumentar su base de datos de direcciones de correo electrónico, que contaba a finales de 2002 con 250 millones de direcciones. Por otra parte, sigue a través de Internet los mensajes enviados, para confirmar que llegan a sus receptores.

En sus mensajes incluye un código tal, que si el mensaje es abierto, envía un mensaje de respuesta. De ahí puede comprobar la efectividad de sus campañas. El 0,33% de los mensajes son abiertos. La tasa de respuestas que consigue en media es del

[170] Este gráfico es el resultado de un experimento que se realizó en 2003 por el UEFF ("United Email Freedom Front"). Información obtenida de www.xtdnet.nl/paul/*spam*/ueff.

[171] "Spam king lives large off others' *e-mail* troubles" (22 de noviembre de 2002), Wendland, M., http://www.freep.com/money/tech/mwend22_20021122.htm.

0,25%, es decir, 625.000 respuestas de los 250 millones de direcciones que contiene su base de datos. Normalmente cobra una comisión por cada venta, pero ha conseguido hasta 22.000 dólares por un único envío a las direcciones de su base de datos completa.

Él dice que no hace nada ilegal, y prefiere llamar a sus mensajes *e-mail* marketing en lugar de *spam*. Asegura respetar el opt-out y ser fiel a la regla de no enviar ningún mensaje con contenido pornográfico. Por ello borra de su base de datos cada día 1.000 direcciones que solicitan no recibir más mensajes publicitarios, y las conserva en otra base de datos que contiene 89 millones de direcciones.

Otras fuentes[172] nos indican que lo que cobra un *spammer* por cada venta que consigue, o por realizar un envío a un determinado número de direcciones de correo electrónico, puede variar mucho. Por ejemplo, según la empresa Symantec un *spammer* medio puede cobrar 1.500 euros por mandar un millón de mensajes.

Los datos con respecto a la tasa de respuesta oscilan desde 0,001% a 0,25% (es decir, de 10 a 250 respuestas por cada millón de mensajes enviados).

Los costes a los que tienen que hacer frente los *spammers*, según la compañía Emarketer[173], son en media de 0,00032 céntimos por cada *spam* enviado, es decir 3,2 dólares por cada millón de mensajes enviados. Si volvemos a las cifras del *spammer* Ralsky, le costaría 800 dólares cada envío a todas sus direcciones de la base de datos. Sin embargo esta cifra (0,00032 ctm/*spam*) es muy optimista. Según otros datos[174], el coste estaría en torno a los 250 dólares por cada 500.000 de envíos (0,05 céntimos por mensaje, aunque esta cifra no sería extensible a más mensajes, puesto que el coste se iría reduciendo cuanto mayor fuera el número de mensajes enviados).

Estas cifras nos hacen llegar a dos conclusiones:

- Las tasas de respuesta del *spam* son muy bajas, pero no lo son tales para que el *spam* no sea rentable, tanto para la empresa anunciante, como para el *spammer*.

- Igualmente, los costes de enviar un *spam* son muy bajos, pero no lo suficiente para que el *spam* sea rentable para cualquier tasa de respuesta o para cualquier negociación de comisión para el *spammer*[175].

Por ello, el *spam* no es rentable para cualesquier negocio o condiciones.

2.2. Origen de las direcciones víctimas de spam.

El primer paso que debe llevar a cabo el *spammer* para realizar su actividad y que da origen a ella, es la obtención de direcciones de correo electrónico de forma masiva. En el apartado 2.2. del bloque II de este trabajo ("Medios y formatos usados por la publicidad en Internet"), se analizaron diversas técnicas a las que acudía el marketing para obtener datos estadísticos de los internautas. Mediante algunas de las técnicas que

[172] "Técnicos y gobiernos sacan la artillería pesada contra el "*spam*"", Molist, M. ((c) 2003), www.aui.es.; "Spam king lives large off others' *e-mail* troubles" (22 de noviembre de 2002), Wendland, M., http://www.freep.com/money/tech/mwend22_20021122.htm.; "For Bulk E-Mailer, Pestering Millions Offers Path to Profit", Mangalindan, M. (The Wall Street Journal, 13 de noviembre de 2002); www.alanluber.com.; "Inside the *spammer*'s world" (29 de junio de 2001), Livingston, B., http://news.com.com; "For Bulk E-Mailer, Pestering Millions Offers Path to Profit" (13 de noviembre de 2002), Mangalindan, M. del Wall Street Journal, http://www.alanluber.com.

[173] "Técnicos y gobiernos sacan la artillería pesada contra el "*spam*"", Molist, M. ((c) 2003), www.aui.es.

[174] Véase el artículo "For Bulk E-Mailer, Pestering Millions Offers Path to Profit" (13 de noviembre de 2002), Mangalindan, M. del Wall Street Journal, http://www.alanluber.com.

[175] Véase el artículo "For Bulk E-Mailer, Pestering Millions Offers Path to Profit".

analizamos se podían recopilar también las direcciones de correo. En este apartado, exponemos más concretamente las tácticas utilizadas especialmente por los *spammers*.

2.2.1. Métodos de captura de direcciones.

Las principales técnicas usadas para la obtención de direcciones con el objetivo de realizar *spam* son la compra de bases de datos selectivas (con direcciones de correo electrónico clasificadas por temáticas de interés), o la elaboración propia, mediante la obtención de las direcciones en listas *opt-in*, páginas *web*, servidores de correo electrónico, búsquedas selectivas en Internet, virus y códigos maliciosos[176]. Los spammres también recopilan direcciones a través de grupos de noticias, listas o foros de discusión, y mensajes encadenados (hoaxes), utilizando normalmente búsquedas selectivas, de forma que los envíos se remiten al grupo de usuarios que lo forman. Explicamos todas ellas a continuación.

- **A partir de listas *opt-in***. Se trata de listas de usuarios que han dado su consentimiento expreso para recibir información publicitaria a cambio de información de interés. Son servicios a los que cualquiera se puede suscribir de forma voluntaria.
- **En sitios *web***. Responsables de sitios *web* sin escrúpulos recogen direcciones de los usuarios que pasan por su portal sin su consentimiento, mediante mecanismos como *web bugs*, *adware*, etc[177]. También de recogen las direcciones de las listas de miembros de *chats*.
- **A través de servidores de correo-e.** Los *spammer* son capaces de extraer direcciones de correo, simulando una transacción SMTP y preguntando si un usuario es o no correcto. Hacen comprobaciones automáticas de nombres de usuario con software combinador, que selecciona nombres posibles para un determinado proveedor de correo, esperando encontrar direcciones válidas entre un conjunto de direcciones de destino aleatorias creadas.
- **Mediante búsquedas selectivas en Internet.** Determinado software especializado es capaz de hacer barridos en Internet o en determinadas zonas para localizar miles de direcciones de correo electrónico.
- **Mediante virus y códigos maliciosos**. Se trata de virus que se propagan por correo electrónico consistiendo su actividad en capturar los datos de la libreta de direcciones del usuario. Contaminan los mensajes y se envían a sí mismos a las direcciones recopiladas para infectar a más usuarios. Posteriormente, se envían a determinadas direcciones para el procesamiento y almacenamiento del material recogido. Este es el caso del virus Sobig[178].
- **A través de grupos de noticias, listas de distribución, foros de discusión y *chats*.** Se remite el *spam* a todas las direcciones incluidas en las listas. En este caso el *spammer* se suscribe al grupo, foro o lista, o bien utiliza la identidad de alguien que

[176] Según Sanz de las Heras, "Evaluación de Alternativas para Reducir el Spam" (mayo 2000), www.rediris.com.

[177] Estas técnicas que obtienen entre otros datos de los internautas su dirección de correo, han sido analizadas en este trabajo en el apartado 2.3 y 3.3. del bloque II ("La obtención de datos estadísticos en Internet con fines de marketing", y "Obtención de datos ilícitos con fines de marketing", respectivamente).

[178] Esta modalidad de recopilación de direcciones de correo electrónico con fines de *spam* fue analizada en el punto 3.1.3.1, "El uso de códigos maliciosos", en el bloque II de este trabajo.

ya está suscrito al mismo. Otra opción es que el *spammer* consiga las direcciones de los miembros del grupo a través de software rastreador.

Esta práctica hace que las listas de distribución, grupos de noticias y foros sean menos útiles para los usuarios, a los que abruman con un aluvión de anuncios y mensajes irrelevantes.

- **Mediante la utilización de hoaxes**. Este método toma especial relevancia por ser los usuarios con su desconocimiento los que facilitan al *spammer* su dirección. Consideramos el tema de especial interés, por lo que dedicamos el siguiente apartado a su explicación.

Las direcciones de correo electrónico que se obtienen mediante los diversos métodos que hemos expuesto, se almacenan y clasifican en bases de datos selectivas con el fin de venderlas o de usarlas posteriormente para realizar *spam*. Conviene destacar que cualquier método de obtención de direcciones de correo sin el consentimiento expreso del usuario es ilegal, ya que la dirección de correo electrónico está considerada en la mayoría de los supuestos como un dato personal por la LOPD[179], con los efectos que ello conlleva en España. Entre otras cosas, prohíbe la compra-venta de direcciones de correo a no ser que se tenga el consentimiento expreso del usuario.

Por ello, el único método legal en España es la elaboración de listas *opt-in*. Sin embargo en los formularios dedicados al efecto, en muchas ocasiones aparece una casilla que dice "No deseo recibir ofertas", que el usuario debería marcar para "en teoría", no dar el consentimiento para recibir comunicaciones comerciales que no sean la que está solicitando. Pero a menudo, el responsable de la gestión de la lista, vende todas las direcciones recogidas, las de los que dieron su consentimiento y las que no. Evidentemente la mayor parte de las listas *opt-in* son legales pero hay mucho engaño e incumplimiento de lo que se asegura en las advertencias de privacidad, además de ser difícil de demostrar cuando existe un incumplimiento.

En contraposición, la legislación de otros países no protege los datos personales de esta manera. En Estados Unidos, por ejemplo, es prácticamente inexistente[180]. De ahí que los *spammers* tengan casi vía libre en este sentido.

Conclusiones interesantes tras el análisis de dos estudios.

Se han analizado dos estudios realizados en la UE[181] y en Estados Unidos[182], que intentan clarificar cuáles son las fuentes de las que los *spammers* se abastecen de

[179] Consultar el apartado 3.1.2.2. del bloque II de este trabajo, "Regulación en España. La LOPD".

[180] Para más información al efecto, consultar el apartado 3.1.2. del bloque II, "Legislación en torno a la protección de datos en Internet", y también el apartado 3.3.2. del este bloque, "Situación en Estados Unidos".

[181] "Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research", realizado por Center for Democracy & Technology de la UE, en marzo de 2003. El estudio ha sido obtenido de www.cdt.org/speech/*spam*/030319spamreport.shtml. Los motivos del informe fueron intentar dar respuesta a la pregunta de cómo los spammers consiguen las direcciones de correo electrónico. El modo de realización del estudio fue exponer en sitios web públicos y listas de noticias más de 250 direcciones creadas al efecto, durante 6 meses. Se recibieron sobre 10.000 mensajes, de los cuales 8.842 fueron *spam*.

[182] Estudio realizado por la Comisión Federal del Comericio de Estados Unidos (FTC), cuyas principales conclusiones han sido tomadas del artículo "Email Address Harvesting: How Spammers Reap What You Sow" (www.ftc.gov). Este estudio se llevó a cabo para descubrir cuáles son los lugares de los que recogen más direcciones en Estados Unidos. Para ello se colocaron 250 nuevas direcciones de correo electrónico en 175 diversas localizaciones de Internet, incluyendo entre ellas páginas web, grupos de noticias y foros, *chats*, mensajería instantánea, y los directorios para páginas web *on line*, nombres de dominio registrados en las bases de datos *whois*, servicios de búsqueda de empleo *on line*, y servicios de

direcciones de correo electrónico. De ambas investigaciones se han obtenido una serie de conclusiones interesantes:

- Los métodos más usados por los *spammers,* son programas de rastreo que buscan direcciones de *e-mail* en áreas públicas de Internet (páginas *web*, de grupos de noticias, listas de distribución, foros de discusión, y *chats*).
- Los sitios más castigados según la FTC fueron los *chats*. Un dato curioso es que una dirección dejada recibía *spam* nueve minutos después de ser utilizada por primera vez. Según el estudio de la UE, las direcciones que recibieron más mensajes no deseados eran las que se habían dejado en sitios *web* de gran afluencia de público.
- El 86% de las direcciones dejadas en páginas *web* recibieron *spam*. No importaba en qué parte del sitio *web* se encontraran siempre que contuvieran el símbolo "@". Las direcciones que se habían ocultado de alguna manera (como no conteniendo este símbolo), no recibieron *spam*[183].
- El 86% de las direcciones dejadas en grupos de noticias, listas de distribución, foros de discusión recibieron *spam* según la FTC. Sin embargo, según el estudio de la UE, estas direcciones reciben algo menos *spam* que las anteriores. Un dato interesante es que las direcciones eran tomadas de las cabeceras de los mensajes de la lista de distribución, en lugar del cuerpo del mensaje.
- Ambos estudios coinciden en que a mayor afluencia de público a un sitio *web* o servicio, más *spam* reciben las direcciones dejadas en él.

Los investigadores encontraron que las direcciones que se incluyeron en otras áreas de Internet, recibieron menos *spam*. La mitad de las direcciones fijadas en páginas *web* personales se mantuvieron libres de *spam*, al igual que el 91% de las direcciones incluidas en directorios de *e-mails*. Las direcciones que se incluyeron en los perfiles de usuario mensajería instantánea, los nombres de dominio registrados en las bases de datos *whois*, los servicios de búsqueda de empleo y búsqueda de pareja *on line*, no recibieron ningún *spam* durante las seis semanas de la investigación de la FTC.

En el estudio de la UE, uno de los dominios fue utilizado por un *spammer* para encontrar direcciones válidas de forma aleatoria, mediante el método "a través de servidores de correo-e", que hemos comentado en este mismo apartado. El servidor atacado, recibió en total 8.506 mensajes, tales como a@nombre_de_dominio, aa@ nombre_de_dominio, aaa@..., aaaa@, b@…, ab@…, aab@…, aaab@…, c@…, ac@…, aac@…, aaac@…, d@…, ad@…, aad@…, aaad@…, etc...

En casi todos los casos, los investigadores encontraron que el *spam* recibido no estaba relacionado con la dirección usada, es decir, que el usuario está expuesto a mensajes *spam* (incluyendo mensajes desagradables) independientemente de su perfil. Esto se puso de manifiesto especialmente en que algunas direcciones de *e-mail* dadas de alta en listas de distribución para niños, recibieron una cantidad grande de *spam* que promovía sitios *web* para adultos, esquemas para trabajar desde casa, e igualan a las otras direcciones en mensajes publicitarios relacionados con las drogas.

búsqueda de pareja *on line*. Después del transcurso de las seis semanas que duró el estudio, las cuentas recibieron 3.349 *e-mails spam*.

[183] Para más información acerca de formas para ocultar la dirección de correo electrónico, consultar el apartado 3.2.1., "Consejos a los usuarios. Pautas para prevenir y minimizar la cantidad de *spam* recibido."

2.2.2. Un método que conlleva además otros graves daños: el hoax[184].

Los hoaxes son mensajes de correo electrónico engañosos, que son distribuidos en cadena por los propios usuarios. Son mensajes no solicitados que por lo general no tienen carácter comercial, pero que llenan el buzón incomodando. En inglés se denominan también *junk mail*, o *garbage mail*.

Los hoaxes se caracterizan por ser enviados desde direcciones no anónimas, por personas que siguen una determinada cadena. Algunos tienen textos alarmantes sobre catástrofes, virus informáticos, noticias que hacen mención a la pérdida del trabajo o incluso a la muerte, que dicen que pueden suceder si no se reenvía el mensaje a todos los contactos de la libreta de direcciones. También hay hoaxes que tientan con la posibilidad de hacerte millonario con sólo reenviar el mensaje, o que apelan a la sensibilidad invocando supuestos niños enfermos. Se basan pues, en el temor o superstición de la gente con el único fin de engañar e intentar recopilar direcciones de correo electrónico para realizar *spam*.

2.2.2.1. Características y categorías de hoaxes.

Los hoaxes tienen en común un objetivo en la gran mayoría de los casos: conseguir direcciones de correo electrónico y congestionar los servidores. En otras ocasiones, su objetivo es alimentar el ego del autor, realizar estafas o difamar a personas.

También tienen en común determinadas características, que pueden ser utilizadas para reconocerlos: no tienen firma (aunque algunos tienen falsas firmas), otros invocan los nombres de grandes compañías, y todos piden ser reenviados a todos los contactos. Generalmente amenazan al receptor del mensaje con grandes desgracias si no lo reenvían, y no remiten a ningún sitio *web* donde comprobar la información.

Por otra parte, el tema al que hacen mención los hoaxes, casi siempre puede ser englobado en alguna de las siguientes categorías[185]:

- Falsas alertas de virus.
- Mensajes de temática religiosa.
- Cadenas de solidaridad. Por un lado juegan con la sensibilidad del receptor ("no pierdes nada reenviando este *e-mail* y un pequeño niño puede salvar su vida"). Por otro lado, perjudican a todas las cadenas que pudieran ser creadas por gente que realmente lo necesita.
- Cadenas de la suerte. Son el equivalente de las viejas cadenas que recibíamos por correo postal ("envíe esta carta a cinco personas. José Pérez no las envió y a la semana murió aplastado por un camión. Nilda Gutiérrez las envió y a los dos días ganó la lotería").
- Leyendas urbanas. Son esas historias que circulan de boca en boca (y en los últimos años a través del correo electrónico) y que mucha gente da por descontado que son ciertas.

[184] La denominación de hoax al mensaje no solicitado de naturaleza no comercial que circula en cadena, ha sido tomada del sitio web www.rompecadenas.com, dedicado a su estudio, y que ha sido adoptado también por la Asociación de Usuarios de Internet.

[185] Según la información obtenida en www.rompecadenas.com.ar. Además, en esta página se pueden encontrar los textos de más de 80 hoaxes, y más detalles de este tipo de práctica.

- Métodos para hacerse millonario, que son el equivalente por correo electrónico, de las clásicas pirámides para hacer dinero.
- Regalos de grandes compañías. Por ejemplo, circulaba uno en el se decía que Microsoft y AOL pagarían una cantidad "x" por cada *e-mail* que se enviara. ¿Cómo pueden saber que yo estoy enviando un mensaje para poder pagarme? Por otro lado, con que unos cuantos miles de personas manden algunos cientos de mensajes, se arruinarían.
- Mensajes tomando el pelo a la gente que envía hoaxes.
- Mensajes verdaderos o están basados en algún hecho real pero que, por diversas causas, no deben ser reenviados en cadena.

Hay otros mensajes que no nacen como hoaxes, pero pueden transformarse en ellos:

- Poemas y mensajes de amor y esperanza (éstos suelen presentarse en un archivo con formato Power Point).
- Mensajes para unirse a programas de afiliados.
- Chistes y fotos que circulan en cadena.

2.2.2.2. Consecuencias que conlleva su distribución y reenvío.

Se podría pensar que las consecuencias del envío de unos cuantos mensajes falsos o mensajes broma son mínimas, o que no pueden llegar a ser dañinos. Pero los hoaxes pueden ser peligrosos por varias razones que comentamos a continuación.

En primer lugar alimentan las bases de datos de los *spammers*, llenan de publicidad y correo electrónico no deseado los buzones de los usuarios, congestionan los servidores, y hacen perder tiempo y dinero al receptor. También hacen ocasionan falta de credibilidad a cadenas creadas por gente que realmente lo necesita.

Por otra parte, determinados hoaxes pueden perjudicar a los usuarios de otras maneras. Por ejemplo, los titulados *Sulfnbk* o *Jdbgmgr*, eran falsas alertas que hicieron que muchísima gente borrara archivos fundamentales en el funcionamiento de Windows creyendo que se trataba de virus.

Muchos hoaxes funcionan en base al miedo que generan y también pueden provocarnos pánico, terror, asco, etc. Sin ir más lejos, la cantidad de hoaxes creados en relación a los atentados en Estados Unidos, generó miedo adicional en mucha gente.

Por otro lado, son especialmente dañinos los mensajes que involucran a personas o empresas reales, ya que es muy fácil utilizar este medio para difamar o calumniar. En efecto, las cadenas de *e-mails* están siendo utilizadas como forma de difamar y ensuciar a competidores o simplemente a alguien a quien se le tiene manía. Un ejemplo de esto es el hoax que vinculaba al grupo musical "La oreja de Van Gogh" con la banda terrorista ETA.

Finalmente, un fenómeno que está apareciendo con mucha frecuencia, es que se toma algún hoax existente y se le insertan todos los datos de alguna persona real (nombre, cargo, lugar de trabajo, teléfono, mail), generalmente profesionales, para darle mayor seriedad al mensaje. No hace falta decir las molestias que esta situación puede causarle a esta persona que aparece avalando supuestamente determinada información (cientos de *e-mails*, llamadas telefónicas, denuncias, etc.). Esta maniobra es una de las más bajas que puedan realizarse: utilizar el nombre de una persona inocente y ajena para difamar a otra. Una vez más, la gente sin escrúpulos se vale de los sentimientos de las personas para hacer daño y recolectar direcciones de *e-mail*.

Por tanto los hoaxes provocan mucho perjuicio, tanto económico como en términos de daños a los internautas. Por un lado recolectan las direcciones de mail, vulnerando la privacidad los usuarios, y por otro, violan la privacidad y el nombre de quienes son víctimas de estas maniobras.

2.2.2.3. Cómo actuar frente a los hoaxes.

No conviene reenviar nunca estos mensajes para no ser cómplice de los *spammers*, ni contribuir a la saturación de los buzones y servidores de correo electrónico.

Si se desea reenviar el mensaje a alguna persona, se debe intentar evitar que circulen todas las direcciones que venían en el mensaje, para que no sean visibles. (Al reenviar un mensaje utilizando la opción "Reenviar mensaje" o "Forward" del programa de correo, automáticamente se incorporan al cuerpo y cabecera del mensaje todas las direcciones incluidas en los campos "Para" y "CC"). Para conseguir que otras direcciones no aparezcan en el mensaje que vamos a enviar, se puede proceder seleccionando la parte del mensaje que se desea reenviar evitando las direcciones, y copiarlo y pegarlo en un mensaje nuevo. También, utilizando el campo "CCO" o "BCC", pues todas las direcciones que se incluyen en estos campos no serán vistas por las personas que reciben el mensaje.

Desde otro punto de vista, hay otros muchos motivos por los que no se deben reenviar estos mensajes, entre ellos, que todos podemos llegar a ser víctimas de estos delincuentes. Imaginemos que el día de mañana vemos nuestro nombre difamado en cientos o miles de *e-mails*. Por ello hay que pensarse varias veces antes de reenviar una cadena que involucra a personas con nombre y apellido, pues se estará siendo cómplice involuntario de la difamación. Por otra parte tampoco conviene reenviar nunca estos mensajes para no ayudar a los *spammers*, ni contribuir a la saturación de los buzones y servidores de correo electrónico.

Los hoaxes son creados por gente sin escrúpulos y difundidos por usuarios honestos que desconocen de qué se trata. Por tanto la mejor forma de romper las cadenas de reenvío de hoaxes es la información y el conocimiento de los usuarios acerca del tema.

No hay una legislación clara frente a estos mensajes de corte no comercial, puesto que se consideran "inofensivos"[186], pero en este apartado hemos dejado claro que deberían estar normalizados al igual que se intenta con los mensajes *spam*. El buzón de correo electrónico puede considerarse como parte de nuestra intimidad, es por ello que un envío no autorizado ni solicitado resulta perjudicial por sí mismo, y por lo tanto atentatorio contra el usuario, que accede a Internet para otras finalidades.

Por eso, y puesto que hoy en día no existe otra forma de combatir esta práctica, es conveniente concienciar a los usuarios de que no sean cómplices y no reenvíen estos mensajes.

[186] Si recordamos los abusos del correo electrónico que explicábamos en el apartado 1.2., (difusión de contenido inadecuado, difusión a través de canales no autorizados, difusión masiva no autorizada, comunicaciones comerciales no solicitadas y ataques con objeto de imposibilitar o dificultar el servicio), observamos que el los hoaxes no están contemplados como abusos del correo electrónico.

2.3. La distribución del spam.

2.3.1. La cadena de distribución del *spam* y sus principales elementos.

Los elementos que forman la cadena de distribución del *spam* son, según Grey, M. C.[187], los siguientes:

- **Proveedores del software** necesario, es decir, gente que se dedica a crear software que hace extremadamente fácil efectuar envíos masivos y buscar direcciones de correo electrónico válidas, asociando combinaciones de letras a nombres de dominio, efectuando potentes búsquedas selectivas en Internet, etc, tal y como comentamos en el apartado anterior.
- **Cosechadores de direcciones**. Se trata de la gente que se dedica a usar el software antes descrito para buscar direcciones de correo electrónico válidas, con las cuales se confeccionan bases de datos.
- **Spammers.** Se trata de las personas que realmente se dedican a enviar los mensajes de forma masiva, utilizando el software apropiado y las bases de datos con las direcciones de destino.
- **Compañías clientes,** es decir, empresas que deciden que las promociones de sus productos y servicios deben llegar a cualquiera, en cualquier lugar, a costa de lo que sea. Por ello deciden hacerlo a través de este método, contratando los servicios de los *spammers*, o realizando el *spam* ellas mismas.
- **Compañías, organizaciones y gobiernos en lucha contra el *spam***, se encuentran en el lado opuesto, intentando y contribuyendo a romper esta cadena.

Todos estos componentes representan una cadena extendida, si bien por la sencillez que implica, en muchas ocasiones todos o varios eslabones son la misma persona o entidad. Dicho lo anterior, podemos analizar cuáles son los principales elementos necesarios para la distribución de *spam*:

- **El software necesario**, que consistiría en buscadores configurados específicamente para encontrar direcciones en Internet, por una parte. Por otra, un programa sencillo que reproduzca un diálogo SMTP, colocando los campos de remite y destino que convengan y falsificando algunas de las cabeceras de tránsito de los mensajes[188].
  Para realizar envíos masivos de *spam* basta con conocer el protocolo SMTP (Simple Mail Transfer Protocol, descrito en el RFC2822), que regula todas las transacciones de correo electrónico de Internet.
- **Una base de datos** con direcciones de correo a las que distribuirá el mensaje de *spam*, que se puede comprar o confeccionar.
- **Una máquina** (estafeta) con la que establecer el diálogo SMTP. En este caso puede ser una máquina local con un paquete de servidor de correo electrónico, o una máquina remota mal configurada a la que se accede por el puerto 25 (SMTP), de forma que permita el encaminamiento de los mensajes que provengan de cualquier dirección IP. En otras ocasiones los *spammers* utilizan métodos de *hacking* para convertir cualquier servidor en un *open relay*.

[187] Grey, M. C., directora de investigación de Gartner Research. Sus declaraciones han sido obtenidas a través del artículo "The Great Spam Supply Chain" (15 de marzo de 2003), www.cio.com/archive/031503/tl_email.html.

[188] Consultar el apartado 2.4., "Análisis de las cabeceras de los mensajes", en el que se analizan cómo y por qué los spammers a menudo falsifican las cabeceras de sus mensajes.

El protocolo SMTP se creó en 1981 de forma insegura para ser usado por científicos, sin pensar en ningún uso comercial. La explosión de Internet en 1994 a nivel social y comercial hizo que se descubrieran los agujeros de SMTP para ser utilizado como el mejor y más barato mecanismo para distribuir y hacer llegar directamente a miles de buzones cualquier tipo de información comercial. Estos agujeros de seguridad de SMTP a menudo pueden solucionarse configurando adecuadamente los servidores de correo electrónico. Sin embargo, hoy en día estos problemas de configuración no están erradicados en el 100% de las máquinas de Internet, por lo que los *spammers* pueden utilizar servidores ajenos para realizar sus envíos masivos. Estos problemas y sus implicaciones se han tratado en el siguiente epígrafe.

2.3.2. El problema e implicaciones de los servidores abiertos.

Los servidores de correo electrónico abiertos o estafetas abiertas (*open relays*) son servidores mal configurados, que permiten a cualquier otra máquina del mundo dirigir mensajes a través de ellos, a otros usuarios de correo de cualquier otra parte de Internet[189]. Esto permite un uso indebido de recursos de la empresa por parte de personas ajenas a la misma. Estas estafetas son las preferidas por los *spammers* para inyectar mensajes *spam*, puesto que de esta forma usan recursos ajenos, cuyos costes no corren a su cuenta. Usando software automatizado, los *spammers* exploran Internet en busca de servidores con estas características. Cuando descubren alguno, encaminan a través de él sus envíos masivos, que son procesados en mayor volumen y menor tiempo de lo que podrían con sus propias computadoras individuales. Este uso indebido, crea problemas a los internautas del mundo entero, a la organización responsable de estas máquinas y a la ejecución de la ley.

Para entender cómo un mensaje ajeno puede ser retransmitido por el servidor de correo electrónico de una organización, es necesario tener presente cómo funciona el servicio de correo electrónico. Cuando alguien de la organización envía un mensaje a un servidor externo, el software del servidor debe comprobar que dicho servidor destino es seguro (si esta definido como tal en sus registros internos). Si es así, enviará el mensaje. Cuando el servidor recibe un mensaje externo, el software deberá confirmar si el receptor del mensaje es un usuario autorizado (perteneciente a la organización), y en ese caso, aceptará la transacción y entregará el mensaje. Si el servidor no es seguro y permanece "abierto", remitirá mensajes a los destinatarios que no son usuarios de la organización y estará configurado de manera que acepta y encamina mensajes a nombre de cualquier usuario de cualquier lugar, incluyendo terceros sin relación. Así, un servidor abierto permite que cualquier remitente, encamine mensajes a través del servidor de la compañía.

Los problemas que esta mala configuración de los servidores de correo electrónico, pueden causar a la organización responsable, se comentan a continuación:

- Los recursos e infraestructuras de comunicaciones pueden ser objeto de hurto y uso fraudulento, pues se está dejando una puerta abierta al uso por terceros desconocidos de los servicios informáticos de la organización.
- Los mensajes *spam* recibidos por terceros pueden parecer provenir del sistema que contiene el servidor abierto. En efecto, el uso de estafetas abiertas permite a los

[189] Consultar el apartado 3.2.3., "Consejos a los PSI y los administradores de servidores de correo electrónico", en el que se abordan consejos a los proveedores de servicio en Internet y a los administradores de servidores de correo electrónico para configurar correctamente los servidores de correo electrónico y así evitar que los spammers puedan usar de forma indebida sus recursos.

spammers encubrir sus identidades, porque parece que el *spam* viene realmente de ellas.

- Si los servidores de una organización en concreto son usados de este modo, el tráfico podría colapsar el sistema. La red de la organización podría verse inundada por los mensajes *spam* que intenta enviar, por quejas de las personas que los reciben, y con el *spam* devuelto de las direcciones que se incluyeron en el envío, pero no existían. La reparación de esta sobrecarga, podría ser costosa y repercutir en una gran cantidad de tiempo fuera de servicio. Pero aún más costosa podría ser la pérdida potencial de confianza de los que piensen que es dicha organización la que ha enviado el *spam*.
- El proveedor de servicios de Internet puede cortarle el servicio al detectar esta práctica.
- Un mayor tráfico, puede provocar que los costes administrativos se incrementen.

Pero esto no es todo, los *spammers* también pueden usar servidores *proxy* abiertos (mal configurados) de la organización. Ello puede permitir situaciones tales como que terceras personas se introduzcan en el sitio *web* de la organización, y se conecten a otras máquinas de Internet desde el interior. Por ejemplo, un *spammer* puede usar un *proxy* abierto para conectarse al servidor de correo electrónico de la organización, cargar el envío masivo de *spam*, y luego desconectarse, todo ello de forma anónima y sin posibilidad de rastreo.

La Comisión Federal del Comercio de Estados Unidos (FTC) asegura que ha detectado al menos 1.000 estafetas que podrían estar potencialmente abiertas, de las cuales el 90 por ciento se encuentran en 16 países: Estados Unidos, China, Corea, Japón, Italia, Polonia, Brasil, Alemania, Taiwán, México, Gran Bretaña, Chile, Francia, Argentina, India, España, y Canadá. Estos países se reflejan en el siguiente mapa.

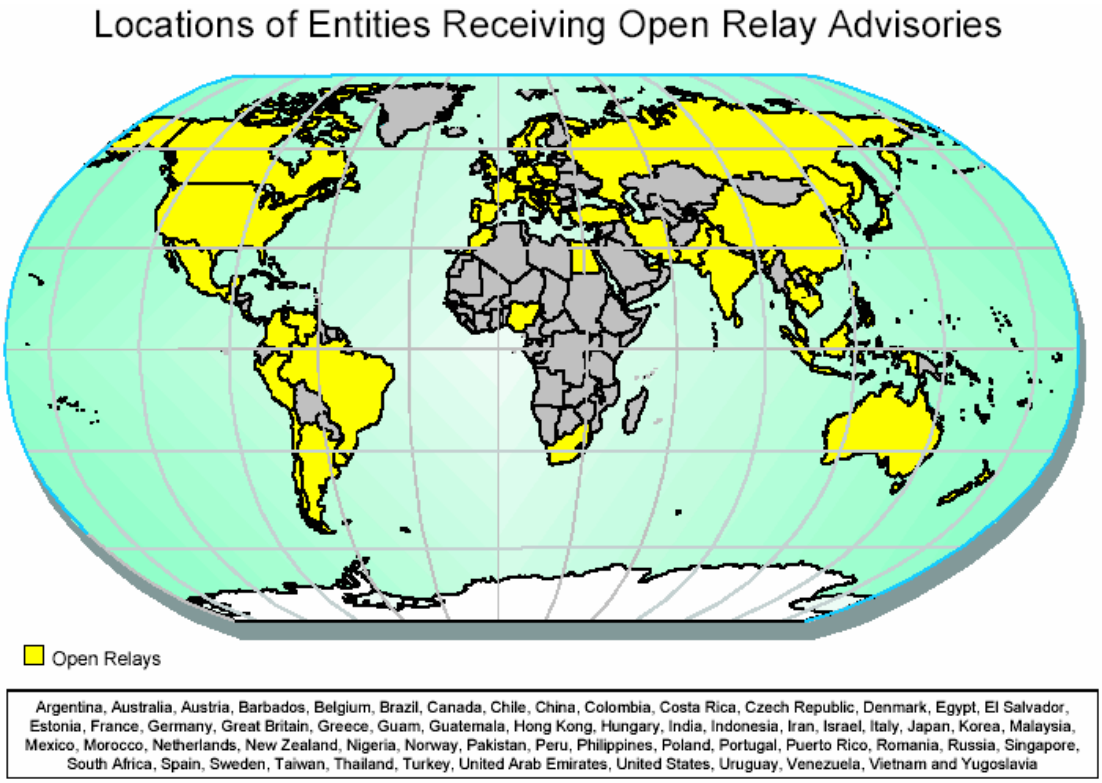

Ilustración 43. Localización de las entidades que reciben avisos por tener los servidores mal configurados (*open relays*). Fuente: FTC (Federal Trade Commission).

El por qué existen tantos servidores mal configurados, se debe principalmente a que en los primeros tiempos de Internet, muchos servidores de correo se mantenían abiertos para permitir que los *e-mails* viajasen entre diversas redes. Esto ayudó a crecer a Internet. Como herencia de esta época algunos servidores poseen por defecto esta configuración abierta, aunque hoy en día, es más probable que sea utilizada por un *spammer*.

2.4. Análisis de las cabeceras de los mensajes.

Los *spammers* intentan ocultar su identidad falsificando las cabeceras de los mensajes de correo electrónico. De hecho, según un estudio realizado por la Comisión Federal del Comercio de Estados Unidos[190], de una muestra al azar de 1.000 mensajes *spam* de entre más de 11 millones, el 44% usó direcciones de retorno falsas para ocultar la identidad del remitente, o un "asunto" engañoso. En este apartado veremos qué son dichas cabeceras, cómo encontrar la verdadera identidad del emisor del *spam* a través de éstas, las herramientas disponibles para localizar las direcciones de Internet de origen, y los datos del proveedor de Internet origen, en los casos en los que sea posible.

2.4.1. Qué son y para qué sirven las cabeceras de los mensajes de correo electrónico.

El servicio de correo electrónico funciona en su forma más simple, en la que sólo se ven implicados dos servidores de correo, del siguiente modo:

- Cuando se envía un *e-mail*, el software del cliente de correo del emisor envía el mensaje a un servidor de correo.
- Éste analiza la cabecera del mensaje y encuentra cual es el dominio al que debe dirigirse (en el caso de la dirección de correo tresmr@hotmail.com, el dominio sería "hotmail.com").
- Conocido el dominio de destino, envía el mensaje a la estafeta de correo encargada de ese dominio para que ella distribuya el mensaje al usuario, en el caso del ejemplo anterior, "tresmr".

En general, en este protocolo pueden participar también uno o varios servidores intermedios, cuya función es la de redirigir el mensaje hasta el servidor de destino.

A continuación mostramos un ejemplo de cabecera, en el que se puede ver cómo está formada por una serie de campos que contienen una serie de información. En el ejemplo, el emisor del mensaje era tresmr@hotmail.com y el receptor, jmmpos@terra.es:

[190] Información obtenida del artículo "Dos tercios del '*spam*' que recibimos son fraudulentos", www.iblnews.com, y del propio estudio: "False Claims in Spam, a report by the FTC's Division of Marketing Practices", abril de 2003. Federal Trade Commission.

Return-Path: *<martammr@mixmail.com>*
Received: *from tsmtp3.ldap.isp ([10.20.4.23]) by mb30.terra.es (terra.es) with ESMTP id HPHCHU00.JC5 for <jmmpos@terra.es>; Sat, 6 Dec 2003 16:32:18 +0100*
Received: *from relay.mixmail.com ([62.151.8.30]) by tsmtp3.ldap.isp (terra.es) with ESMTP id HPHCHS00.RVX for <jmmpos@terra.es>; Sat, 6 Dec 2003 16:32:16 +0100*
Received*: from [172.30.8.15] (helo=web01) by relay.mixmail.com with smtp id 1ASePn-0007dj-00 for jmmpos@terra.es; Sat, 06 Dec 2003 16:32:15 +0100*
Date: *Sat, 06 Dec 2003 16:32:15 +0100*
From: *"Marta Martin-Moreno Redondo" <martammr@mixmail.com>*
Reply-To*: martammr@mixmail.com*
To: *"jmmpos@terra.es" <jmmpos@terra.es>*
Subject: *de mixmail*
Xmailer*: Mixmail Server 3.0*
X-Priority: *3*
MIME-Version: *1.0*
Content-type: *text/plain*
Content-Transfer-Encoding: *quoted-printable*
Message-Id: *<E1ASePn-0007dj-00@relay.mixmail.com>*

Ilustración 44. Ejemplo de cabecera de mensaje de correo electrónico.

Los datos que contienen los distintos campos de la cabecera, incluyen información sobre:

- el origen y el emisor del mensaje (*"Return-Path:", "Received:", "Reply-To:" y "From:"*),
- el receptor (*To:*),
- el tipo de mensaje (*"Content-Type:"*),
- el programa que el remitente utiliza para el correo electrónico (*"Xmailer:"*)
- la versión del protocolo que se usa ("*Mime-Version:"*)
- las fechas en que se envió el mensaje y se recibió (*"Date:" y "X-OriginalArrivalTime:"* respectivamente),
- y los distintos servidores de correo que participan en el servicio (*"Received:"*), también llamados estafetas o relays, por donde el *e-mail* ha circulado desde que se envió, hasta que llegó al buzón de destino.

La forma de visualizar las cabeceras de un mensaje de correo electrónico depende del gestor de correo que se utilice, pero todos lo permiten. Así, por ejemplo si se usa Outlook Express, se puede hacer señalando el mensaje y pulsando "Control-F3".

2.4.2. Cómo interpretar la cabecera de un mensaje.

Ya hemos comentado qué información se incluye en los diversos campos que forman la cabecera, pero el campo que nos interesa para intentar averiguar la identidad del *spammer* es "*Received:*". Cada estafeta por la que pasa el mensaje, añade una

información en la parte de arriba de este campo, de tal manera que el primer campo "*Received:*" ha sido añadido por la última estafeta por donde pasó el mensaje, y el último, debería indicar la primera estafeta que recibió el mensaje, suponiendo que no se han usado técnicas de enmascaramiento, es decir, que no se ha falsificado parte de la cabecera o que el servidor de origen incluye información en este campo[191]. Según el mensaje va pasando por diversas estafetas hasta llegar al destinatario, se añaden campos "Received". Así, el esquema del campo "*Received:*" para una secuencia de estafetas A->B->C->D es:

Received: from <estafeta_que_manda(C)> by <estafeta_que_recibe(D)><datos>.
Received: from <estafeta_que_manda(B)> by <estafeta_que_recibe(C)><datos>.
Received: from <estafeta_que_manda(A)> by <estafeta_que_recibe(B)><datos>.

Es decir, se lee de abajo a arriba y de izquierda a derecha para recomponer la secuencia. Los servidores B y C son estafetas intermedias entre las de origen y destino (A y D respectivamente).

Reproducimos a continuación el campo "*Received:*" del ejemplo anterior para clarificar que significa cada componente:

Received: from tsmtp3.ldap.isp ([10.20.4.23]) by mb30.terra.es (terra.es)
with ESMTP id HPHCHU00.JC5 for <jmmpos@terra.es>;
Sat, 6 Dec 2003 16:32:18 +0100
Received: from relay.mixmail.com ([62.151.8.30]) by tsmtp3.ldap.isp (terra.es)
with ESMTP id HPHCHS00.RVX for <jmmpos@terra.es>;
Sat, 6 Dec 2003 16:32:16 +0100
Received: from [172.30.8.15] (helo=web01)by relay.mixmail.com
with smtp id 1ASePn-0007dj-00 for jmmpos@terra.es;
Sat, 06 Dec 2003 16:32:15 +0100

Esta cabecera es de un mensaje legítimo (y por tanto con su cabecera no falsificada), enviado desde martammr@mixmail.com a jmmpos@terra.es, que indica que el mensaje original fue mandado desde una máquina cuya dirección IP es [172.30.8.15] (que pertenece a Mixmail), que ha pasado por dos servidores intermedios, "relay.mixmail.com", con dirección [62.151.8.30], "tsmtp3.ldap.isp" (Terra.es), con dirección [10.20.4.23], y que fue entregado a "mb30.terra.es" (Terra.es).

A continuación vamos a ver dos mensajes de correo, que provienen de *spammers*, cuya cabecera ha sido falsificada. Un indicio de que el mensaje o su cabecera ha sido falsificados, es si se observa que se rompe la secuencia de estafetas del campo "*Received:*". Los datos que aparezcan tras este punto de ruptura pueden ser falsos.

[191] Existen todavía servidores de una versión antigua de SendMail, que no registran esta información, por lo que si el *spammer* usa este tipo de servidor, no podremos rastrear su mensaje. Sin embargo, afortunadamente no es el caso más habitual.

Mensaje 1: La siguiente cabecera es de un mensaje *spam* dirigido a la dirección de correo tresmr@hotmail.com.

X-Message-Info: ASZdpiY8olkOLMeOyu9AxQlar2pq6Aw6/Muu/W3TUsQ=
Received: from mc7-f26.hotmail.com ([65.54.253.33])
by mc7-s11.hotmail.com with Microsoft SMTPSVC(5.0.2195.6713);
Fri, 5 Dec 2003 12:25:50 -0800
Received: from ôÉàæÄãÄÜ×öÐ©Ê²Ã´£ ([80.139.98.148])
by mc7-f26.hotmail.com with Microsoft SMTPSVC(5.0.2195.6713);
Fri, 5 Dec 2003 12:25:49 -0800
To: <Oraqgcvpobr6Wt2LH791@yahoo.com>
From: "Liz" <tomblikecontributoryboatyard@tombstonecontrite.net>
Subject: -=SIZE=- it D0es matter
Date: Fri, 05 Dec 2003 15:26:05 -0500
MIME-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Return-Path: tomblikecontributoryboatyard@tombstonecontrite.net
Message-ID: <MC7-F26rx5zAa6l3zZx0000835b@mc7-f26.hotmail.com>
X-OriginalArrivalTime: 05 Dec 2003 20:25:50.0320 (UTC)
FILETIME=[F932EF00:01C3BB6D]

Ilustración 45. Primer ejemplo de cabecera falsificada que pertenece a un mensaje *spam*.

Observamos inicialmente que algunos campos de la cabecera contienen ristras de caracteres extraños. Así, el campo "*To*:" (dirección de destino) no contiene la verdadera dirección de destino (que es tresmr@hotmail.com), sino una dirección extraña (Oraqgcvpobr6Wt2LH791@yahoo.com). El campo "*From*:" y el nombre de la máquina de origen (en el campo "*Received:*") también da la impresión de que se han falsificado.

Mensaje 2: Veamos un segundo mensaje *spam*, que también iba dirigido a tresmr@hotmail.com.

X-Message-Info: 8Q6ATcAEb5e7zPw0COqY18Hn5ysiSxR1Ta5EkS16Z2g=
Received: from mc8-f8.hotmail.com ([65.54.253.144])
by mc8-s13.hotmail.com with Microsoft SMTPSVC(5.0.2195.6713);
Wed, 3 Dec 2003 15:24:55 -0800
Received: from Zcotierwymtn3F ([80.139.48.158])
by mc8-f8.hotmail.com with Microsoft SMTPSVC(5.0.2195.6713);
Wed, 3 Dec 2003 15:24:36 -0800
To: <faarabnqh6LR3Dr575@hotmail.com>
From: "Tammy Wolf" <nowherescrimmage.org>
Subject: View it before its gone
Date: Wed, 03 Dec 2003 18:24:48 -0500
MIME-Version: 1.0
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Return-Path: nowherescrimmage.org@mail.hotmail.com
Message-ID: <MC8-F89wmfKGezPLC6M0001d6b2@mc8-f8.hotmail.com>
X-OriginalArrivalTime: 03 Dec 2003 23:24:37.0334 (UTC)
FILETIME=[9E2BDF60:01C3B9F4]

Ilustración 46. Segundo ejemplo de cabecera falsificada que pertenece a un mensaje *spam*.

En este segundo mensaje tampoco coincide el contenido del campo "*To*:" con la dirección de destino. Sin embargo observamos que el nombre de la máquina origen en el campo "*Received:*" (Zcotierwymtn3F), sí podría corresponderse con una máquina real.

En ambos mensajes, a pesar de la falsificación de la cabecera, vemos que ésta nos da información de los servidores por donde ha transitado el mensaje antes de llegar al buzón de destino y la verdadera dirección IP del servidor de origen, que sirve para localizar el sitio desde el que el *spammer* está haciendo sus envíos masivos. Esta dirección IP se encuentra al principio del último campo "*Received:*", la cual en el primer mensaje es [80.139.98.148], y en el segundo, [80.139.48.158].

2.4.3. Herramientas para localizar a los responsables del servidor origen del *spam*.

Dada la dirección IP de origen de los mensajes, podemos optar de diversas maneras para tratar de combatir el *spam*. Se puede efectuar una queja al encargado de la gestión del sitio *web* con esa dirección, que normalmente debería ser postmaster@80.139.98.148 o abuse@80.139.98.148, en el caso del primer mensaje analizado en la sección anterior.

También se puede localizar qué sitio *web* es el que tiene asignada dicha dirección, y con ello, los datos del responsable. Existen varias vías que pueden ayudarnos a ello. Para obtener el nombre de dominio de una dirección IP, se puede

hacer una consulta a un servidor DNS. Ésta se puede efectuar mediante herramientas al efecto, dependiendo del sistema operativo que se use, o si no se dispone de ninguna, se puede acudir a páginas que facilitan estos accesos, como www.dnsstuff.com.

Para obtener datos de un dominio o de una dirección IP, como la dirección de correo electrónico de su responsable, se pueden utilizar las bases de datos *whois* de dominios de Internet: base de datos InterNIC (www.internic.net/cgi-bin/whois), para dominios *.edu, .com, .org*, y *.net;* RIPE NCC (www.ripe.net/db/whois.html), para dominios europeos, o la base de datos del ES-NIC (https://www.nic.es/esnic/servlet/WhoisControllerHTML), sólo para dominios *.es*.

En la página *web* antes mencionada, www.dnsstuff.com, se nos ofrecen herramientas para poder consultar todas las bases de datos necesarias de forma transparente, así como otras herramientas útiles para rastrear una dirección IP o un nombre de dominio, o saber si está incluida en una de las 300 listas negras de *spammers* a las que puede acceder la página en cuestión.

Una dirección IP, como hemos dicho, caracteriza unívocamente una máquina en Internet, pero ésta puede ser estática, como en el caso de servidores o de conexiones mediante ADSL, o dinámicas dentro de un rango asignado por un servidor. En el caso de que la dirección sea dinámica, también nos hará falta saber la fecha y hora en que se envió dicho mensaje, que viene reflejada en el campo "*Date*:".

Para los mensajes *spam* analizados anteriormente, cuyas direcciones origen hemos descubierto que eran [80.139.98.148] y [80.139.48.158], tras realizar una consulta a las bases de datos *whois*, obtenemos que ambas pertenecen a la misma organización cuyos datos son los siguientes[192]:

[192] (C) Copyright 2000-2003 Computerized Horizons, obtenido de www.dnsstuff.com.

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:        80.128.0.0 - 80.146.159.255
netname:        DTAG-DIAL16
descr:          Deutsche Telekom AG
country:        DE
admin-c:        DTIP
tech-c:         DTST
status:         ASSIGNED PA

remarks:
**************************************************
remarks: *ABUSE CONTACT: abuse@t-ipnet.de
remarks:* IN CASE OF HACK ATTACKS, ILLEGAL ACTIVITY,
          * VIOLATION, SCANS, PROBES, SPAM, ETC.
**************************************************
mnt-by:         DTAG-NIC
changed:        ripe.dtip@telekom.de 20010807
changed:        ripe.dtip@telekom.de 20030211
source:         RIPE

route:          80.128.0.0/11
descr:          Deutsche Telekom AG, Internet service provider
origin:         AS3320
mnt-by:         DTAG-RR
changed:        bp@nic.dtag.de 20010807
source:         RIPE

person:         DTAG Global IP-Addressing
address:        Deutsche Telekom AG
address:        D-90492 Nuernberg
address:        Germany
phone:          +49 180 5334332
fax-no:         +49 180 5334252
e-mail:         ripe.dtip@telekom.de
nic-hdl:        DTIP
mnt-by:         DTAG-NIC
changed:        ripe.dtip@telekom.de 20031013
source:         RIPE

person:         Security Team
address:        Deutsche Telekom AG
address:        Germany
phone:          +49 180 5334332
```

fax-no:	*+49 180 5334252*
e-mail:	*abuse@t-ipnet.de*
nic-hdl:	*DTST*
mnt-by:	*DTAG-NIC*
changed:	*abuse@t-ipnet.de 20030210*
source:	*RIPE*

Ilustración 47. Resultado de la consulta de la dirección [80.139.98.148] a la base de datos *whois*. (C) Copyright 2000-2003 Computerized Horizons, obtenido de www.dnsstuff.com.

De todos estos datos, nos interesa conocer la base de datos que contenía esta dirección, que era RIPE; la dirección de correo electrónico a quien podemos enviar nuestra queja, que es abuse@t-ipnet.de; y los datos de la organización: una descripción de su nombre y actividad ("*Deutsche Telekom AG, Internet service provider"*), el país de origen (*Germany*) y un número de teléfono y fax de contacto.

3. Medidas preventivas contra el *spam*.

3.1. Introducción.

En este apartado vamos a exponer algunas medidas para prevenir el *spam*. Primero, desde el punto de vista de una serie de consejos a distintos agentes que de alguna manera participan o son víctimas de actividades relacionadas con el *spam*. Estos consejos pueden ayudar a los usuarios a recibir menos *spam*, y a que éste sea menos perjudicial para ellos. También se aportan consejos a los administradores de correo electrónico, para que por un lado informen a los usuarios sobre el tema, y por otro, controlen sus sistemas y sus políticas institucionales, para evitar que los recursos que gestionan sean mal utilizados por sus propios clientes o por *spammers* ajenos al servicio.

En segundo lugar, se incluye un análisis sobre la situación legislativa en relación al *spam* en la Unión Europea y en Estados Unidos. La legislación también puede considerarse una medida preventiva contra el *spam*, pues lo que persigue en último término es la imposición de multas y penas para disuadir a los *spammers* de que lleven a cabo sus actividades. La legislación, es pues una medida preventiva, aunque se aplique con posterioridad a que las actividades de *spam* se hayan producido.

En mayor o menor cuantía, estas medidas de prevención contra el *spam* son necesarias y si fueran ampliamente adoptadas, podrían contribuir si no a una erradicación del problema, sí a una disminución de la cantidad de *spam* que circula. Por tanto en mi opinión, es de gran importancia conocerlas y cumplirlas en la medida de lo posible para luchar contra este problema.

3.2. Consejos para prevenir el spam.

En esta sección vamos a aportar una serie de consejos para prevenir y ayudar a combatir el *spam*. Los hemos dividido en consejos a los usuarios, consejos a los creadores de contenidos, foros, listas y páginas *web*, y consejos a los proveedores de servicio y los administradores de servidores de correo electrónico.

Desde cada una de estas tres perspectivas, intentaremos aportar cuáles son las consideraciones básicas que deben tenerse en cuenta, sin pretender entrar en demasiado nivel de detalle. Veámoslos pues, comenzando por los consejos a los usuarios.

3.2.1. Consejos a los usuarios. Pautas para minimizar la cantidad de *spam* recibido.

El seguir la serie de pautas que comentamos a continuación, nos puede ayudar a minimizar la cantidad de *spam* recibido en nuestras cuentas de correo, así como a mantener unas ciertas buenas costumbres en relación con la seguridad de nuestros datos.

Para la redacción de este apartado se ha consultado a varias organizaciones que luchan contra el *spam*, así como a entidades gubernamentales nacionales, como la Agencia de Protección de Datos[193], e internacionales, como la Comisión Federal del Comercio de Estados Unidos. Veamos pues cuales son estas recomendaciones.

1. No hacer pública la dirección de correo electrónico, siempre que sea posible, en las páginas *web*, las listas de distribución, *chats*, etc. Pues aunque la dirección deje de ser pública, o ya no se use un determinado *chat* o lista, las direcciones pueden seguir siendo utilizadas por los *spammers*.

Si hay que suministrar la dirección, pueden tenerse en cuenta algunos de estos consejos, que dificultarán que la dirección llegue a manos de *spammers*.

- Se puede suministrar una dirección de correo electrónico temporal gratuita, distinta de la que se usa normalmente, con el fin de que nos sea fácil prescindir de ella en el caso en que ya no nos interese.
- Los métodos de rastreo de direcciones de los *spammers* se basan a menudo la búsqueda del carácter "@", que contienen todas las direcciones de *e-mail*. Si omitimos este carácter, lo sustituimos por "ARROBA", o incluimos "QUITALASMAYUSCULAS" después de "@", reduciremos drásticamente las posibilidades de que nuestra dirección sea captada por los *spammers*. Vemos un ejemplo con la dirección de correo tresmr@hotmail.com: siguiendo este procedimiento, la haríamos pública como "tresmrARROBAhotmail.com" o "tresmr@QUITALASMAYÚSCULAShotmail.com" (si fuera imprescindible incluir el carácter "@"). En efecto, los resultados de un reciente estudio realizado[194] indican que si la dirección se oculta de alguna manera, aunque sea sencilla como las que acabamos de enunciar, las posibilidades de recibir *spam* por la captura de la dirección mediante programas rastreadores (que es la principal fuente de los *spammers*), es prácticamente nula.

2. Leer y comprender la política de privacidad y los formularios de los sitios *web* donde se suministre la dirección de correo electrónico u otros datos. La información es en muchas ocasiones la mejor arma de los consumidores electrónicos. Puesto que en España la LOPD no permite la utilización de datos personales (la dirección electrónica puede ser calificada como dato personal)[195], ni su uso por terceros sin previa autorización, los sitios *web* que pretendan hacer uso de la dirección de *e-mail* facilitada por los usuarios, deben advertirlo al menos en su política de privacidad.

Por ello, en el caso de que no existan otras advertencias, se debe poner atención en comprender la política de privacidad, pues muchos sitios se basan en redactarlas muy extensas para que los usuarios no se molesten en leerlas. En cualquier caso, si ésta no aparece, permite a la compañía vender la dirección de correo electrónico, cederla a terceros, o va a realizar algún uso sospechoso, o con el que no se esté de acuerdo, es mejor no facilitarla, o al menos valorar si nos interesa hacerlo pese a todo.

En el caso de formularios, se debe marcar (o desmarcar) alguna casilla, en el caso de que exista, en la que se especifica que no se desean recibir comunicaciones comerciales. De cualquier modo conviene entender lo que se advierte en éste.

[193] En los anexos a este trabajo, se adjuntan las recomendaciones que da la Agencia de Protección de Datos a los usuarios en este ámbito. Se consideran de interés, por lo que se recomienda su consulta en este punto.

[194] "Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research" (www.cdt.org/speech/*spam*/030319spamreport.shtml), realizado por Center for Democracy & Technology de la UE, en marzo de 2003. Las direcciones estudiadas que fueron ocultadas de alguna manera no recibieron ningún *spam*, frente a los más de 8.000 que recibieron otras direcciones sometidas al estudio.

[195] La LOPD y en particular lo que dicta en torno a la dirección de correo electrónico se analizó en el apartado 3.1. del bloque II de este trabajo.

3. Usar más de una dirección de correo electrónico dependiendo del uso que se vaya ha hacer de ella. Esto ya lo apuntábamos en la primera pauta, y con ello queremos recalcar que es ventajoso disponer varias direcciones de correo según sea el uso que vayamos a darle: una para los mensajes personales, otra para asuntos profesionales, otra para proporcionarla en *chats* u otros sitios *web* con fines de ocio, por ejemplo.

4. Elección de la dirección de correo electrónico. La dirección marta@dominio.com, por ejemplo, es posible que reciba más cantidad de *spam* que otra como m_x5_r1@dominio.com. En efecto, si se usa un nombre poco común como dirección de *e-mail*, es más difícil que le llegue *spam* con direcciones de destino aleatorias, que suele ser uno de los métodos utilizados por los *spammers*. Así, éstos utilizan combinadores que seleccionan nombres posibles y palabras de diccionario, para un determinado proveedor de correo, esperando encontrar direcciones válidas[196].

5. Usar al menos las opciones de filtrado del gestor de correo. Todos los gestores de correo actuales incluyen algún tipo de herramientas para filtrar mensajes y bloquear direcciones concretas, de tal forma que no se reciban mensajes de ellas.

La mayoría de proveedores que ofrecen cuentas de correo electrónico *web* gratuitas, poseen herramientas específicas contra el *spam*. Por ejemplo, Ya.com (Mixmail) ofrece la posibilidad de configurar filtros de correo no deseado dependiendo del grado de seguridad que se requiera para la cuenta (alta, media y baja), y envía los mensajes calificados como *spam* a una carpeta específica. Hotmail y Yahoo! también poseen herramientas parecidas para combatir el *spam*.

En el caso de uso de gestores de correo como Outlook, Eudora, etc, que todavía no incluyen herramientas específicas, siempre podemos instalar alguna. En el apartado 4.5.1.1. ("Desde el punto de vista del usuario"), analizaremos qué herramientas existen y cuáles son adecuadas en cada caso.

3.2.2. Consejos a los creadores de contenidos, foros, listas y páginas *web*.

La mayor parte de los sitios *web* en Internet combaten el *spam* adoptando sus propias medidas de protección y vigilancia. No obstante, independientemente de la actividad que se lleve a cabo, es conveniente seguir unos consejos básicos para prevenir y combatir el *spam* tanto para las direcciones propias del responsable de la página *web*, de los internautas que la visiten, así como de sus clientes.

En general, no se deben publicar direcciones de correo en las páginas, a no ser que sea estrictamente necesario. Si se publican direcciones, se deben tomar algunas medidas de precaución para que éstas no sean rastreadas por los *spammers*. Para dificultar que una dirección sea tomada, se puede recurrir a sencillas técnicas que las hacen invisibles a los programas de rastreo. Estas técnicas están basadas en que estos programas funcionan haciendo búsquedas selectivas de las "arrobas" o el "mailto" que aparecen en las direcciones. Una manera puede ser publicar las direcciones en formato de gráfico, sin el enlace al *e-mail*. También se puede implementar una función en *Javascript*, tal que dado únicamente el nombre del buzón, le añada la arroba y el nombre de dominio para completar la dirección de correo. De esta forma en la página sólo aparece el nombre del buzón, por lo que no puede ser tomada automáticamente.

[196] Consultar el apartado 2.2., "Origen de las direcciones víctimas de spam", donde se explica y se ilustra con un ejemplo este método obtención de direcciones de los spammers.

Otra forma podría ser incluir la dirección ASCII codificada en decimal, o sustituir la arroba por otro texto, como hemos comentado en el apartado anterior de consejos a los usuarios.

En el caso de gestión de listas de distribución, se debe disponer de las medidas mínimas para proteger el servicio:

- No se deben permitir altas sin que se validen a través de la dirección de correo electrónico suscrito, para evitar altas no deseadas a terceros. Es una buena práctica, incluir en los mensajes siempre un enlace que permita darse de baja de ella de forma sencilla, con el fin de controlar la disponibilidad de la relación de los suscriptores.
- Si la lista posee contenidos accesibles, es conveniente no publicar los *e-mails* de los participantes en los mensajes que se publican, o advertir de los riesgos que conlleva la participación.
- Es muy positivo que antes de publicar los mensajes, éstos pasen por algún sistema de moderación o validación, para evitar mensajes comerciales o mensajes *off-topic*.
- No permitir listas públicas de envío.
- Controlar y limitar el número máximo de copias o envíos simultáneos que pueden realizar los que utilizan los servicios, con el fin de evitar envíos masivos desde la lista.

A continuación incluimos una serie de consejos que se han de tener en cuenta si el sitio *web* que se gestiona obtiene la dirección de correo de sus usuarios, con el fin de enviarles información promocional sobre dicho sitio *web*. Se ha de ser muy cuidadoso para que el sitio *web* goce de confianza y no sea calificado como *spammer*, con las consecuencias que ello traería al respecto.

3.2.2.1. Aspectos a tener en cuenta al solicitar o recoger datos a los usuarios.

Cuando un usuario se suscribe a una página *web* porque le interesan servicios que en ella se ofrecen o información sobre sus productos, es interesante que se le informe de la finalidad y las condiciones en las que serán tratados sus datos en el mismo formulario de suscripción, con el objetivo de que el usuario de su consentimiento con la mayor información posible al respecto. Para que el usuario no se vea sorprendido, es conveniente también incluir otra información sobre la periodicidad aproximada de los comunicados o boletines que se le va a enviar, quien es el responsable de los datos que suministra, así como si éstos se cederán a terceros. También debemos asegurarnos de que el consentimiento sea explícito, para evitar que usuarios que acepten sin leer las advertencias.

Estas prácticas son positivas para ambas partes, ya que por un lado se está actuando de forma ética, honesta y legal de acuerdo con las leyes de protección al consumidor y de protección de datos, y por otra, los usuarios se sentirán seguros y tendrán confianza, repercutiendo esto en una mayor fidelidad de los suscriptores y mayor eficacia de las comunicaciones que sean enviadas.

3.2.2.2. Validación de los datos.

Una práctica que también reporta beneficios a ambas partes es comprobar los datos de los usuarios tan a fondo como sea posible, con el fin de no utilizar datos incorrectos de algún usuario, y con ello mejorar la calidad de los boletines enviados y

sus contenidos. En especial, la dirección de correo que se recibe a través de cualquier medio anónimo, como puede ser un formulario en una página *web*.

Es positivo analizar los datos (nombres y direcciones sobre todo) y preguntarse cuántos de ellos son realmente válidos. Aunque la ventaja del correo electrónico es que los costes de los envíos son muy inferiores a los envíos postales, existe la falsa creencia de que tiene menos importancia el envío masivo sin la validación de los datos. Para conseguir saber si los datos son válidos, se puede enviar un mensaje de validación con un enlace para completar el proceso de alta. De esta manera se garantizará la validez de los datos, eliminar las posibles direcciones erróneas y desde el punto de vista de combatir el *spam*, hacer del boletín una herramienta útil y segura que otorgará calidad al servicio.

Algunos de los obstáculos o inconvenientes del proceso de validación, tienen que ver con que un 30% de los clientes potenciales no completan el proceso de alta. Aunque este dato pudiera llevar a la no utilización un sistema de validación, se debe pensar que es más positivo disponer de una lista de clientes más pequeña, pero con el 100% de los datos correctos, que de una lista mayor con un 30% de clientes con sus datos erróneos.

De esta forma y mandando boletines sólo a clientes potenciales cuyos datos y consentimiento sean cien por cien veraces, se conseguirán más clientes reales y sin ningún riesgo de perder la conexión del proveedor de servicios por ser calificado de *spam* o ser incluido en una lista negra, con las molestias que ello conllevaría.

3.2.2.2. Adquisición de listas de direcciones de terceros.

La venta de datos sin el consentimiento expreso del usuario al que pertenecen está prohibida en España por la LOPD. Se debe por tanto ser reacio a la compra de direcciones, pues en la mayoría de las ocasiones éstas direcciones no han sido tomadas con el consentimiento de los usuarios que las forman para disponer de ellas, o sus datos son erróneos. En el caso de compra, se debe pues solicitar los formularios de autorización de los usuarios, así como su política de privacidad.

La consecuencia de enviar *e-mails* de promoción a usuarios obtenidos de una lista comprada, que no haya sido correctamente confeccionada en el sentido que venimos aconsejando, será que se enviará información a receptores que no leerán los contenidos de los mensajes, o simplemente no les llegará porque la dirección no era correcta. Sin contar con las quejas de los usuarios que no solicitaron esos envíos, por la invasión a la intimidad o acusando de realizar *spam*.

3.2.3. Consejos a los PSI y los administradores de servidores de correo electrónico.

3.2.3.1. Recomendaciones.

Los proveedores de servicio y los administradores de servidores de correo electrónico, deben comprometerse a favorecer la confianza de los usuarios en Internet, e intentar evitar el abuso de terceros de los recursos de que disponen, por el beneficio de

ambas partes, usuarios y compañía. Para ello la entidad debe tener en cuenta una serie de recomendaciones que se detallan a continuación[197].

1. Se debe disponer de una política institucional para el uso correcto de los recursos de la red (dominio y rango de direcciones IP asignadas) que delimite sus responsabilidades. En ella se ha de tener en cuenta que la institución debe responsabilizarse del servicio de correo electrónico que se ofrezca a instituciones autorizadas (dominios residentes, fundaciones, organismos independientes, etc.), a las que se deberá explicar y deberán aceptar las condiciones de uso. En el apartado siguiente, abordaremos unas pautas sobre cómo debe efectuarse su definición (consultar el epígrafe "Correcta definición de una política institucional para el uso del servicio de correo electrónico").
2. Se deben tomar las medidas mínimas de seguridad para evitar abusos de los recursos de la compañía. Por ello, la institución tiene que garantizar que todos los servidores de correo electrónico de su red están adecuadamente configurados y cumplen con unas determinadas pautas que garantizan la seguridad. En el apartado siguiente (epígrafe "Configuración adecuada de los servidores de correo") se detallan algunas de las más importantes.
3. En caso de que la institución disponga de foros o listas de distribución, debe disponer de unas medidas mínimas para proteger el servicio, que han sido comentadas en el apartado anterior, con los consejos a los creadores de páginas *web*, foros, y listas de distribución.
4. En el caso de recabar datos de carácter personal o direcciones de correo electrónico, se debe proporcionar mecanismos para que el usuario pueda ejercer sus derechos de rectificación y cancelación de los mismos (según lo especificado en la LOPD), así como de informar de la forma de llevarlo a cabo. Hay que tener en cuenta que la institución es responsable de las consecuencias que impliquen el almacenamiento y manipulación automática de datos de direcciones de correo electrónico por parte de los usuarios de su red. Al igual que en la recomendación número 3, los consejos sobre este tema han sido abordados en la sección anterior.
5. Se deben atender las quejas y comunicaciones de los usuarios, y se debe garantizar que se gestionan los incidentes que llegan al buzón <abuse@dominiodelaempresa.es> a los buzones o formularios que la empresa disponga para este fin, actuando de la manera que corresponda según el caso.
   La institución debe dar a conocer la existencia de dichas direcciones, e indicar el tipo de información que es necesario enviar para poder tomar acciones, y documentándola en su caso. Además, debe por lo menos considerar, y contestar a las quejas y denuncias que lleguen a dicho buzón, sean locales o externas. Así, cuando se ha demostrado un incidente de abuso interno, la institución se debe comprometer a tomar las medidas oportunas contra el involucrado de acuerdo con la política de uso correcto de la red de dicha institución y la legislación vigente.
6. La institución debe garantizar que los actuales y futuros usuarios con dirección de correo electrónico del dominio interno, son informados de manera clara, comprensible, y de fácil localización sobre los siguientes aspectos:
   - Identificación de la empresa o proveedor. Según lo dispuesto en la LSSI sobre los prestadores de servicios de la sociedad de la información, se deben incluir todos los datos de la compañía[198].

[197] Muchas de estas prácticas son las recomendadas por Sanz de las Heras, J., responsable del servicio de correo electrónico del organismo RedIris (www.rediris.com).

[198] Consultar el apartado 3.1. del bloque II de este trabajo, en el que se especifican las obligaciones que tienen los prestadores de servicios de la sociedad de la información.

- Dirección de correo electrónico o postal donde los usuarios puedan hacer saber al administrador o responsable incidentes o quejas. También los datos que se deben adjuntar para que puedan ser debidamente atendidos.
- Implicaciones del uso del correo electrónico con direcciones del dominio de la institución.
- La política de uso correcto de los recursos y los servicios de la empresa, que ésta adquiere con los usuarios y que desea hacer pública, así como las acciones que se llevarán a cabo en caso de incumplimiento.
- La política de seguridad y privacidad, en la que la compañía deberá explicar el tratamiento y uso que hace de los datos que obtiene (direcciones IP, *cookies*, direcciones de correo y otros datos).
- Los conceptos básicos y efectos de los abusos del correo electrónico, así como enlaces a las instituciones que la compañía crea oportuno para generar confianza en los usuarios, como por ejemplo, a la agencia de protección de datos, cuerpos de seguridad u organizaciones de consumidores.

3.2.3.2. Medidas.

El proveedor de servicio y los administradores de servidores de correo electrónico, pueden intentar prevenir el *spam* desde tres distintos frentes, que ya han sido mencionados en las recomendaciones anteriores, pero que aquí pasamos a comentar más en profundidad.

Correcta definición de una política institucional para el uso del servicio de correo electrónico.

La política institucional se trata de un documento público y fácilmente accesible desde las páginas *web* de la organización, avalado por un responsable de máximo nivel, en el que la organización se debe asegurar de que los usuarios tengan información sobre los abusos del correo electrónico que pueden llevarse a cabo, sus implicaciones y problemática; garantizar que este servicio sea utilizado de acuerdo con unas mínimas normas éticas, y en general asegurar un correcto servicio. Con ella se persigue que la organización sea calificada como "fiable" en este sentido de cara al exterior.

Los objetivos de la política institucional deberían estar ligados a un documento de "términos y condiciones de uso", el cual no tendría objetivos jurídicos sino sólo un compromiso formal, público y activo para luchar y perseguir dentro de sus posibilidades cualquier abuso local y externo referido al problema del *spam*. Además, debe apuntar cuáles serán las posibles medidas técnicas contra usuarios que hayan cometido cualquier infracción relacionada con los abusos que estamos tratando.

La redacción de estos documentos es de gran importancia, sin embargo, según un estudio realizado por la compañía Sybari[199], sólo una tercera parte de las compañías europeas dice tener redactado un documento interno de definición de *spam* para su empresa, de las cuales sólo la mitad lo ha puesto en práctica dándolo a conocer a sus

[199] El estudio realizado por la compañía Sybari a más de un centenar de compañías de dieciséis países, entre los que figura España, y cuyas conclusiones han sido obtenidas del artículo "Las empresas creen que las leyes contra el *spam* son insuficientes" (12 de noviembre de 2003), www.vunet.com.

trabajadores y departamentos. En el otro extremo, el 28 % ni siquiera tiene prevista su emisión.

La organización RedIris propone un ejemplo de documento tipo para la "política institucional" de una organización de la Comunidad RedIris y de un "documento de términos y condiciones de uso", pero que con las correcciones pertinentes podría ser de aplicación para cualquier institución. Se adjuntan a continuación[200] en las dos siguientes ilustraciones.

Política institucional acerca del problema del ACE (Abusos del Correo Electrónico).

Nuestra organización reconoce los principios de libertad de expresión y privacidad de información como partes implicadas en el servicio de correo electrónico. Nuestra organización ofrece unos niveles de privacidad similares a los que se ofrecen en el correo postal tradicional y en las conversaciones telefónicas.
Nuestra institución anima al uso del correo electrónico y respeta la privacidad de los usuarios. Nunca de forma rutinaria se realizarán monitorizaciones o inspecciones de los buzones sin el consentimiento del propietario del buzón asignado por los responsables de nuestra organización. Sin embargo podrá denegarse el acceso a los servicios de correo electrónico locales e inspeccionar, monitorizar y cancelar un buzón privado:

- *Cuando haya requerimientos legales.*
- *Cuando haya sospechas fundadas de violación de la política interna de la institución, como comercio electrónico, falsificación de direcciones etc. Evitando caer en rumores, chismorreos u otras evidencias no fundadas y previo consentimiento del máximo responsable del servicio.*
- *Cuando por circunstancias de emergencia, donde no actuar pudiera repercutir gravemente en el servicio general a la comunidad.*

Disposiciones generales.

1. *Nuestra institución es responsable de cualquier nombre de dominio, DNS de tercer nivel, bajo el dominio "org.es".*
2. *Dentro de los servicios de comunicaciones que nuestra institución provee, se ofrece un buzón de correo electrónico y una o varias máquinas para el encaminamiento y recogida de correo a/desde Internet a todo nuestro personal que lo requiera. Teniendo registro de las personas que los están utilizando bajo las direcciones electrónicas de las que somos responsables.*
3. *Como gestores del servicio de correo electrónico dentro de nuestra institución, nos reservamos el derecho de tomar las medidas sancionadoras oportunas contra los usuarios internos y externos que realicen cualquiera de los abusos incluidos en el Anexo 1.*
4. *Disponemos de suficiente información acerca de:*
   - *Las diversas actividades que trascienden los objetivos habituales del uso del servicio de correo electrónico que presta nuestra Institución (Anexo 1).*
   - *Los perjuicios directos o indirectos que este problema ocasiona a nuestros propios usuarios, rendimientos de máquinas, líneas de comunicaciones, etc, reflejados en el Anexo 2.*

[200] Fuente: www.rediris.es/mail/abuso.

Objetivos.

Este documento ha sido escrito con los siguientes objetivos en mente:

1. *Proteger la reputación y buen nombre de nuestra institución en la Red (Internet).*
2. *Garantizar la seguridad, rendimientos y privacidad de los sistemas de nuestra organización y de los demás.*
3. *Evitar situaciones que puedan causar a nuestra organización algún tipo de responsabilidad civil o penal.*
4. *Preservar la privacidad y seguridad de nuestros usuarios.*
5. *Proteger la labor realizada por las personas que trabajan en nuestros servicios de comunicaciones frente a ciertos actos indeseables.*

Ámbito de aplicación.

1. *Todas las máquinas de nuestra institución capaces de encaminar correo electrónico (estafetas).*
2. *Todas las piezas de mensajes (texto, cabeceras y trazas) residentes en ordenadores propiedad de nuestra institución.*
3. *Todos los usuarios responsables de buzones asignados por los responsables de nuestra organización.*
4. *Todos los servicios internos que utilizan el correo electrónico, como por ejemplo los servidores de listas de distribución y respondedores automáticos.*

Esta política sólo se aplica al correo electrónico en formato electrónico y no es aplicable a correo electrónico en formato papel.

Compromisos

1. *Emplear los recursos técnicos y humanos a nuestro alcance para intentar evitar cualquiera de los tipos de abusos reflejados en el Anexo 2.*
2. *Poner a disposición pública y fácilmente accesible de nuestros usuarios, propietarios de buzones institucionales, de la siguiente información:*
   - *"Términos y condiciones de uso del servicio de correo electrónico" (se adjunta a continuación).*
   - *"Abuso del correo electrónico y sus implicaciones".*
3. *Poner a disposición de los usuarios del servicio de correo electrónico de la institución los procedimientos adecuados para que puedan actuar contra los abusos externos del correo que sufrirán en sus propios buzones (correo basura o spamming).*
4. *Intentar mantener nuestros servidores de correo institucionales con las últimas mejoras técnicas (actualizaciones, parches, filtros, etc.) para defenderlos de los ataques definidos en el Anexo 1.*
5. *Proteger los datos personales de nuestros usuarios: nombre, apellidos y dirección de correo electrónico de acuerdo a la legislación española reflejada en la LORTAD (Ley Orgánica de Tratamiento de Datos - Ley Orgánica 5/1992 del 29 octubre) .*
6. *Intentar impedir y perseguir a usuarios internos que realicen cualquiera de las actividades definidas en el Anexo 1.*
7. *Coordinarnos con el equipo gestor del Programa RedIRIS para colaborar en la creación de un frente común frente a este tipo de actividades definidas en el Anexo 1. Esto incluye la colaboración al nivel necesario para la persecución de estas actividades*

8. *Dedicar un buzón (abuse@organizacion.es) donde puedan ser enviados y atendidos los incidentes.*

Aprobado por el Director de la organización.

Ilustración 48. Ejemplo de documento tipo para la política institucional en relación con el problema del abuso del correo electrónico de una organización. Fuente: www.rediris.es/mail/abuso.

Términos y condiciones de uso del correo electrónico.

En apoyo de los objetivos fundamentales de nuestra institución: enseñanza e investigación y respetando los principios de libertad de expresión y privacidad de información, se ofrece un serie de recursos de red, comunicaciones y de información a nuestra comunidad. El acceso a estos recursos es un privilegio que está condicionado a la aceptación de la Política de Utilización de estos recursos. Se debe reconocer que la calidad de estos servicios depende en gran medida de la responsabilidad individual de los usuarios.
En caso de no entender completamente alguno de estos apartados póngase en contacto con el responsable del servicio en le teléfono 9xxx o el buzón postmaster@org.es. Las condiciones que se exponen pueden ser actualizadas para acoplarse a nuevas situaciones.

1. *Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y su buzón asociado en nuestra organización.*
2. *Es una falta grave facilitar y/o ofrecer nuestra cuenta y buzón a personas no autorizadas.*
3. *Los usuarios deben ser conscientes de la diferencia de utilizar direcciones de correo electrónico suministradas por nuestra institución, o privadas ofrecidas por cualquier proveedor Internet. El campo remite de las cabeceras de correo indica el origen al que pertenece el emisor de un mensaje, por lo que hay que tener en cuenta las repercusiones. Resumiendo, para temas privados deben ser usados los buzones del proveedor Internet, pero nunca desde las instalaciones de nuestra organización y para temas profesionales serán usadas las direcciones de nuestra organización.*
4. *Correo personal. Los servicios de correo electrónico suministrados por nuestra organización pueden ser usados de forma incidental para temas personales excepto si:*
    - *interfieren con el rendimiento del propio servicio,*
    - *interfieren en las labores propias de los gestores del servicio,*
    - *suponen un alto coste para nuestra organización.*

Los mensajes de tipo personal están sujetos a los términos y condiciones de este documento.

5. *Debe de ser consciente de los términos, prohibiciones y perjuicios englobados en el documento "Abusos del Correo Electrónico".*
6. *Está prohibida la utilización en nuestras instalaciones de buzones de correo electrónico de otros proveedores Internet:*

- *Es ilegal utilizar como encaminador de correo otras máquinas que no sean las puestas a disposición por nuestra organización.*
- *Es incorrecto enviar mensajes con direcciones no asignadas por los responsables de nuestra institución y en general es ilegal manipular las cabeceras de correo electrónico saliente.*

7. *El correo electrónico es una herramienta para el intercambio de información entre personas no es un herramienta de difusión de información. Para ello existen otros canales más adecuados y efectivos, para lo que debe de ponerse en contacto con los responsables del servicio.*
8. *La violación de la seguridad de los sistemas y/o red pueden incurrir en responsabilidades civiles y criminales. Nuestra organización colaborará al máximo de sus posibilidades para investigar este tipo de actos, incluyendo la cooperación con la Justicia.*
9. *No es correcto enviar correo a personas que no desean recibirlo. Si le solicitan detener ésta práctica deberá de hacerlo. Si nuestra organización recibe quejas, denuncias o reclamaciones por estas prácticas se tomarán las medidas sancionadoras adecuadas.*
10. *Está completamente prohibido realizar cualquiera de los tipos de abusos definidos en el documento "Abusos del Correo Electrónico". Además de las siguientes actividades:*
    - *Utilizar el correo electrónico para cualquier propósito comercial o financiero.*
    - *No se debe participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares.*
    - *Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra organización.*
    - *Está prohibido falsificar las cabeceras de correo electrónico.*
    - *Las cuentas de nuestra organización no deben ser usadas para recoger correo de buzones de otro proveedor de Internet.*
11. *Estará penalizado con la cancelación del buzón, el envío a foros de discusión (listas de distribución y/o newsgroups) de mensajes que comprometan la reputación de nuestra organización o violen cualquiera de leyes españolas*

Aprobado por el Director de la organización.

Ilustración 49. Ejemplo de documento tipo para los términos y condiciones de uso del correo electrónico de una organización. Fuente: www.rediris.es/mail/abuso.

Configuración adecuada de los servidores de correo.

La correcta configuración de los servidores que proporcionan el servicio de correo electrónico, ayudará a proteger el sistema de usos indebidos de los recursos informáticos de la organización por parte de *spammers*. Uno de los problemas que representa una mala configuración de los servidores ya fue tratada en este trabajo[201], sin

[201] El tema de los servidores abiertos fue tratado en el apartado 2.3.2., donde se puede encontrar información sobre qué se entiende como servidor abierto, y cuáles son sus implicaciones. En el apartado 3.2.3. ("Consejos a los PSIs y a los administradores de servidores de correo electrónico), se explica

embargo aquí se pretende profundizar en cuáles son las pautas a seguir para solucionar estos problemas de abusos no autorizados de terceros. Una buena forma de comprobar si una organización tiene los servidores de correo electrónico mal configurados, puede ser mediante el sitio *web* www.mail-abuse.org/tsi, donde se puede encontrar abundante documentación sobre los pasos a seguir dependiendo del sistema operativo y del software que se tenga instalado.

El servidor principal de correo electrónico de una organización debe ser el centro del servicio, desde el cual se coordine la seguridad de todo el servicio en la organización. Los requisitos recomendables[202] a tener en cuenta para configurarlo desde el punto de vista de la seguridad, se detallan a continuación.

1. Definir el espacio de direcciones de correo lógicas de las que es responsable el servidor, sin omitir los dominios virtuales.
2. Definir claramente las direcciones IP de las redes a las que se da servicio de correo electrónico, y que deberán ser las únicas que tengan permiso de utilizar el servidor principal para encaminar *e-mails*. A cualquier otra se le debe denegar el servicio de la transacción SMTP.
3. No aceptar *e-mails* desde direcciones externas y destinadas a direcciones externas al dominio de la organización. Este principio junto con el anterior, debe denegar el encaminamiento de mensajes de correo electrónico desde cualquier dirección IP exterior, destinada a cualquier dirección IP exterior, independientemente de cual sea la dirección de origen que aparezca en el campo "*mail from:*". De esta forma nos aseguramos de que los servidores no estén abiertos, es decir, que evitan el encaminamiento de forma no autorizada a terceros.
4. Comprobar las resoluciones DNS para rechazar conexiones SMTP de servidores que no dispongan de resolución inversa, y para rechazar mensajes en los que durante la sesión SMTP aparezca un valor de "*mail from:*" con un dominio incorrecto.
5. Implementación de listas de acceso de direcciones de dominios, usuarios y/o direcciones que se les deniega el acceso, por no tener protegido su servidor de correo, por ser máquinas de proveedores de servicio que dan soporte a *spammers*, o por ser máquinas que hacen *spam*; así como disponer de herramientas para filtrar estas direcciones.
6. Limitar el número de mensajes que un usuario puede enviar por minuto y comprobar periódicamente el número total de mensajes que se envían desde cada uno, para evitar que un *spammer* se aloje entre nuestros usuarios.
7. Configurar los servidores para que proporcionen códigos de error normalizados y almacenar la identidad de las máquinas (dirección IP), e información correcta y suficiente donde se reflejen las trazas de todas las transacciones SMTP, así como la fecha correcta de los envíos. Se debe conservar durante un tiempo razonable estos ficheros y revisarlos y actualizados de forma periódica. Con estas medidas se podrán depurar y mejorar los errores que se presenten, garantizar que los *e-mails* generados dentro de la red pueda ser identificado y seguido hasta su origen, así como identificar prácticas fraudulentas.

De este modo no se debe permitir el encaminamiento desde o a servidores terceros que no pertenezcan a la organización. Con ello se habrá solucionado este problema y no se estará siendo cómplice de *spammers*.

detalladamente cómo configurar adecuadamente los servidores para que éstos no puedan ser usados por terceros de forma fraudulenta.

[202] Según la institución RedIris, www.rediris.es.

3.3. Legislación.

La legislación se encuentra desde mi punto de vista entre una de las medidas preventivas de lucha contra el *spam*, puesto que lo que se persigue en último fin con su creación y aplicación, es intimidar con sanciones las actividades del *spam* para evitar que se produzcan en la medida de lo posible.

En este apartado, se analizará desde el punto de vista específico del *spam* la legislación que concierne al tema, sobre todo en el ámbito internacional (básicamente de EEUU y de la UE), aunque también se hará un análisis crítico de la situación en nuestro país, intentando complementar el resumen sobre legislación relativo a la publicidad, a la protección de datos y a los delitos informáticos realizado en el apartado 3.1 del bloque II de este trabajo ("Breves apuntes sobre legislación y códigos éticos en la Red.").

3.3.1. Situación en la UE[203].

En el bloque II de este trabajo se resumieron los principales puntos de la Directiva 2000/31/CE, que afecta a las comunicaciones comerciales, y que llevaron a la aprobación en España de la LSSI. Sin embargo, en relación directa con la lucha contra el *spam* la UE aprobó la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas), que prohíbe el envío de comunicaciones comerciales no solicitadas a personas físicas en toda la Unión Europea. La normativa se basa en el principio de consentimiento previo (*opt-in*)[204], además de que todos los mensajes deben mencionar una dirección de respuesta válida donde el abonado pueda oponerse al envío de mensajes posteriores. Además, todos los mensajes enviados a direcciones conseguidas sin conocimiento de los destinatarios son considerados ilegales y cada Estado miembro puede imponer multas por ello. La única excepción que se tiene en cuenta es el caso del marco limitado de las relaciones entre clientes y empresas. En este caso se autorizan las comunicaciones con el cliente siempre que este haya mantenido una relación con la firma y no haya manifestado expresamente su oposición a recibir este tipo de menajes.

Esta directiva europea debía ser transpuesta a la legislación nacional de cada estado con fecha máxima de octubre de 2003, sin embargo Bruselas se ha visto obligada a abrir procedimientos de infracción contra países como Francia, Bélgica, Holanda, Luxemburgo, Portugal, Finlandia, Suecia y Alemania por no haber cumplido los plazos previstos para introducir a escala nacional esta normativa. De esta forma, a fecha enero de 2004, los países que han adoptado una legislación que prohíbe el *spam* mediante un régimen *opt-in* son Dinamarca, España, Grecia, Italia, Finlandia, Alemania, Bélgica,

[203] La información necesaria para redactar este apartado ha sido obtenida de la página www.eurocauce.org, portal de lucha legal internacional contra el *spam*, del portal de la Comisión Europea, www.europa.eu.int/pol/infso/index_es.htm, y de varios artículos: "La UE anuncia medidas contra el '*spam*' por la desconfianza que causa" (27 de enero de 2004), Europa Press, www.elmundo.es/navegante; "¿Spam sí o *spam* no? Legalidad" (26 de agosto de 2003), Hernández, J., www.baquia.com; "La Comisión Europea declara la guerra al *spam*" (23 de enero de 2004), www.vunet.com; "Bruselas contra el '*spam*'", Reuters, www.elmundo.es/navegante; "En Gran Bretaña el envío de SPAM es un delito" (19 de septiembre del 2003), http://www.conocimientosweb.net/dt; "Legisladores británicos planean extraditar a quienes envíen *spam*" (30 de octubre del 2003), www.conocimientosweb.net/dt; "Europa prohibirá el *spam* a partir de otoño", Sánchez, Y., www.diarioenred.com.

[204] Los términos opt-in y opt-out, fueron adecuadamente explicados en el apartado 3.1.2.1. del bloque II de este trabajo ("Clarificación del significado e implicaciones de los términos opt-in y opt-out"). Por tanto se remite a él para mayor claridad, o al glosario de términos.

Austria y el Reino Unido, de las cuales Finlandia, Alemania y Bélgica, sin embargo todavía no han adoptado todas las competencias de la mencionada directiva.

La ley contra el *spam* del Reino Unido, que entró en vigor el 11 de diciembre de 2003 ha levantado gran controversia, puesto que ha incluido la posibilidad de poder extraditar a los *spammers* que envíen mensajes a usuarios del Reino Unido desde otros países para poder ser juzgados allí. Sin embargo ha sido criticada porque impone una pena máxima de 5.000 libras esterlinas (9.255 dólares). Los expertos señalan que no es disuasoria, puesto que algunos de ellos obtienen de 20.000 a 30.000 libras (de 37.020 a 56.030 dólares) por semana por realizar los envíos masivos y en Estados Unidos por ejemplo, se ha indemnizado a compañías como American Online, con casi siete millones de dólares por daños en un caso de *spam*.

La controversia levantada por esta ley en el Reino Unido es tan solo un ejemplo del debate que está teniendo lugar en todo el mundo alrededor de este tema. Veamos a continuación cuál es la situación en España.

3.3.1.1. Situación en España.

En el bloque II de este trabajo[205] se incluyó un breve análisis de la legislación española encuadrada en la europea sobre temas relacionados con Internet y las comunicaciones comerciales. Allí se expuso el contenido de la LSSI que concierne a la prohibición de las comunicaciones comerciales no solicitadas, pero en un contexto más amplio. En este punto se pretende hacer un análisis crítico desde el punto de vista de su aplicación y su eficacia en la lucha contra el *spam*.

La legislación española contempla, regula y penaliza las actividades de *spam* en el contexto de la LSSI (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico), en el Título III, de "comunicaciones comerciales por vía electrónica". Tras su entrada en vigor, como se comentó, se prohibía totalmente el envío de *spam* en España. Sin embargo, y posteriormente a esta legislación, se han introducido unos cambios en la Ley General de Telecomunicaciones (LGT, aprobados a 16 de diciembre de 2003) que afectan a la LSSI. En la disposición primera, modificación del artículo 21, permite la utilización del correo electrónico para remitir mensajes a aquellas personas o empresas con las que se haya mantenido una relación contractual sin necesidad de una autorización previa por parte de estas. Textualmente dice lo siguiente: "*Lo dispuesto en el apartado anterior (referente a la prohibición de envíos comerciales) no será de aplicación cuando exista una relación contractual previa"*.

Según fuentes del Ministerio[206] esta "redefinición" del concepto de *spam* tuvo lugar por la necesidad de adaptarse a la normativa europea en este sentido (Directiva 2002/58/CE), que autoriza las comunicaciones con el cliente siempre que este haya mantenido una relación con la firma y no haya manifestado expresamente su oposición a recibir este tipo de menajes. Esta nueva formulación, satisface también a las peticiones que desde distintas asociaciones empresariales vinculadas al comercio electrónico se realizaron en tal sentido, ya que éstas se encontraban con la imposibilidad legal de informar a sus clientes de las promociones y ofertas por correo electrónico, mientras desde fuera de nuestro país, se bombardea a sus clientes con todo tipo de proposiciones.

[205] Consultar el apartado 3.1.1. del bloque II, "Legislación en torno a la comunicación o promoción *on line*".

[206] Esta información ha sido obtenida de los artículos "La Fecemd advierte sobre la legislación de *e-mails* publicitarios" (09-12-2003, www.fecemd.org) y "El *spam* a los clientes será legal en España"; www.noticiasdot.com.

Sin embargo, esta nueva situación hace que un tipo de *spam* sea legal en España, no conservándose en sentido estricto la opción del usuario de no recibir ningún tipo de mensaje no solicitado sin consentimiento explícito previo. La opinión de que debe prohibirse todo tipo de *spam*, es compartida por usuarios[207], asociaciones de empresas de marketing interactivo, y organismos de lucha contra el *spam*. Para evaluar adecuadamente la situación, pensemos en las bases de datos de las que disponen las grandes empresas con las que cualquier ciudadano se ve obligado a contratar los suministros básicos: Telefónica, Fecsa-Endesa, Iberdrola, Gas Natural, Bancos y Cajas de Ahorros, etc. En la actual situación legislativa, dichas empresas lo sucesivo quedan legitimadas para inundar el buzón de correo electrónico del usuario, ofreciéndole productos o servicios de su propia empresa que sean similares a los inicialmente contratados. Y del mismo modo, y en virtud del principio de igualdad, cualquier otra empresa, sea multinacional o pyme, empezando por aquellas que nos ofrecen acceso a Internet. Esto derivará en una gran cantidad de mensajes.

Por otro lado, el gran problema que se presenta independientemente de la situación legislativa española concreta, es que dado el carácter internacional del *spam*, la legislación nacional no es muy efectiva para evitar el problema dentro de España. En efecto, teniendo en cuenta que al conectarse a Internet se rompe toda forma de fronteras, se pueden delimitar puntos de origen pero no puntos de encuentro o puntos de paso de la información, es decir, una persona en Hong-Kong usando una cuenta de correo *web* de un proveedor de servicios en Argentina, puede enviar un mensaje *spam* a usuarios en "n" países (de manera simultanea), entre ellos a uno que tiene su cuenta en un servidor español. En un caso cómo éste, aunque la víctima del *spam* sea española, no se puede acudir a la LSSI, ni a las directivas europeas. Por ello, la legislación nacional es necesaria, pero no demasiado útil para prevenir o combatir el *spam*, ya que sólo puede regular las emisiones de *spam* con origen en máquina ubicadas en territorio nacional.

Es de destacar en este punto, que aunque la legislación española prohíba el *spam* en casi todas sus formas, los datos que barajamos en el apartado 2.2.2.3. de este trabajo ("Origen del *spam* por países"), mostraban que a fecha de marzo de 2003, España estaba entre los 10 primeros países productores de *spam*. Este dato nos obliga a reflexionar sobre la eficacia de la situación legislativa actual.

3.3.1.2. Opinión de las empresas.

En relación a lo anterior, recogemos aquí la opinión al respecto de las empresas, según varios estudios[208]. Por un lado, a finales de 2002 (tras la aprobación de la LSSI sin ninguna modificación), se observa que en España la mayoría de las empresas

[207] Según el estudio realizado por la entidad Transatlantic Consumer Dialogue (TACD), la mayoría de los internautas cree que el *spam* debería ser prohibido y que la única forma de comunicación comercial mediante correo electrónico legal debería ser el opt-in. El estudio es "Consumer Attitudes Regarding Unsolicited Commercial Email (Spam)", realizado en octubre-diciembre de 2003, por la entidad Transatlantic Consumer Dialogue (TACD) a 21.102 internautas, de 36 países entre los que figura España.

[208] Se han tenido en cuenta los resultados de dos estudios. El "IV Estudio sobre el Marketing y la Publicidad Medios Interactivos 2002", realizado por AGEMDI-fecemd" (Asociación de Agencias de Marketing Directo e Interactivo-Federación Española de Comercio Electrónico y Marketing Directo) a 258 empresas españolas anunciantes/usuarias de publicidad con más de 11 empleados independientemente de su sector de actividad de forma aleatoria, que dirigen sus productos y servicios al consumidor final. Y el estudio realizado por la compañía Sybari a más de un centenar de compañías de dieciséis países, entre los que figura España, y cuyas conclusiones han sido obtenidas del artículo "Las empresas creen que las leyes contra el *spam* son insuficientes" (12 de noviembre de 2003), www.vunet.com.

consultadas consideran aceptable la legislación que afecta a sus comunicaciones interactivas en ese momento (un 49%), lo que muestra una falta de opinión crítica al respecto causada por el desconocimiento general acerca del tema, aspecto que se pone aún más de manifiesto dado que casi un tercio de las empresas consultadas (31%) no sabe o no contesta ante esta pregunta. Algo parecido ocurre respecto a la pregunta de que si han disminuido sus acciones de marketing *on line* a causa de la ley. La ley no ha afectado a casi ninguna empresa y un 30,6% de las empresas tampoco sabe o no contesta a esta pregunta, por lo que podemos apreciar cómo el desconocimiento de la nueva legislación de Internet sigue siendo algo llamativo y preocupante.

Estas cifras ponen de manifiesto que realmente la entrada en vigor de esta ley no ha redundado en importantes trabas a las empresas que llevan a cabo pulicidad *on line*.

Por otro lado, según un estudio realizado por la compañía Sybari en 2003, la mitad de las empresas europeas considera que la actual legislación sobre las comunicaciones electrónicas no afectará en absoluto a la recepción masiva de *e-mails* comerciales no solicitados vía Internet. Así, revela que apenas una de cada veinte empresas cree que la acción de los reguladores pondrá fin al *spam*, mientras que una de cada cinco augura una reducción de esta práctica. En la misma línea, casi la mitad de las compañías encuestadas desconfían completamente de que sus gobiernos vayan a implantar una legislación contra el *spam* eficaz, considerando el porcentaje restante que tan sólo tendrá una eficacia limitada.

Estos datos ponen de manifiesto que las empresas no creen que la legislación de sus países vaya a ser una herramienta eficaz de lucha contra el *spam*, ya sea porque su naturaleza no sea la adecuada, o porque una legislación no sea la solución al problema.

3.3.2. Situación legislativa en Estados Unidos[209].

La situación legislativa en torno al *spam* en Estados Unidos hasta finales de 2003 era un tanto caótica, puesto que cada estado había sido libre de adoptar sus propias medidas o de no hacer nada al respecto. El resultado había sido que existían estados con una legislación contra el *spam* incluso demasiado estricta, como en Carolina del Sur, donde un *spammer* podía enfrentarse a condenas de veinte años de cárcel si se aplicaba rigurosamente la ley, y estados donde no existía ley alguna.

La solución a este caos fue aprobar la ley federal "Controling the Assault of Non-Soclicited Pornography and Marketing Act. of 2003" (CAN-SPAM Act.), el 16 de diciembre de 2003, que crea a partir del 1 de enero de 2004 una situación uniforme para el marketing por *e-mail* y propone penas para un conjunto de actividades relacionadas con el *spam*, como el robo o la obtención de direcciones electrónicas de sitios *web*. Esta es la primera iniciativa de reglamentación de contenidos en Internet en Estados Unidos desde sus inicios en los años 90 y ha sido aprobada tras conocer los resultados del

[209] Gran parte de la información requerida para la elaboración de este apartado ha sido obtenida de la página web www.spamlaws.com y www.ftc.gov, además de los artículos "El Congreso de USA aprueba ley 'anti-*spam*'" (24 de noviembre del 2003), www.conocimientosweb.net/dt; "EEUU limita el *spam*" (24 de noviembre de 2003), www.vunet.com; "Legisladores de Estados Unidos legalizan el *spam*" (27 de noviembre del 2003), http://www.conocimientosweb.net/dt; "Estados Unidos aprueba ley de regulación del Spam" (02/12/2003), Guillem Alsina, http://diariored.com; "Multan a un '*spammer*' con 93.000 euros tras aceptar los cargos" (14 de mayo de 2003), www.iblnews.com; "Internautas, empresas y legisladores se unen contra la plaga del correo basura" (22 de mayo de 2003), www.iblnews.com; y del estudio "Spam E-mail and Its Impact on IT Spending and Productivity" (diciembre de 2003), Spira, J. B., realizado por Basex Inc., www.basex.com.

estudio realizado por la FTC[210] (Federal Trade Commission), en el que se advertía de que la mayoría de los mensajes eran fraudulentos y de la existencia de abundantes mensajes con material pornográfico.

Así, el objetivo principal de esta ley, como comprobaremos en este apartado, no es propiamente combatir el *spam*, sino erradicar los mensajes pornográficos y fraudulentos. Por tanto, en lo esencial la ley legaliza el *spam*: permite a cualquier sujeto o empresa enviar publicidad masiva, hasta que el propio usuario solicite ser dado de baja en la lista. Este principio de "solicitud activa de baja en la lista" (opt-out) se contrapone totalmente al principio de "solicitud activa de alta en la lista" (*opt-in*), aprobado anteriormente en algunos estados como California. El problema para California, al igual que para otros estados que ya habían dictado leyes contra el *spam*, es que éstas han quedado sin efecto tras la entrada en vigor de la CAN-SPAM, debido a que ésta se trata de una ley federal.

Veamos pues lo que implican los puntos más destacados de esta ley:

- A partir de la entrada en vigor de esta ley el 1 de enero de 2004, se prohíben los **envíos masivos con remitente falso**, una práctica habitual entre los *spammers*. En esta situación el usuario afectado no puede responder, darse de baja de la lista, o emprender algún tipo de acción contra el remitente. En caso de incumplir esta norma, se puede ser sancionado con penas de prisión de hasta 3 años.
- El renglón de **asunto del mensaje** deberá hacer referencia explícita al contenido de éste. Esta obligación viene de que muchos *spammers* envían a los internautas mensajes con asuntos como "*Re:*" o "*Re: Your password*", con la intención de confundirlos y hacer que abran los mensajes.
- Se limita el envío de publicidad referida a **contenidos pornográficos**, que solamente se podrá hacer con una marca que diseñará la FTC (Federal Trade Commission).
- Permite **opt-out**: el aspecto más polémico de la ley es que permite a las empresas enviar publicidad masiva a cualquier usuario hasta que éste se de de baja de la lista de distribución. Este principio choca frontalmente con el que piden la mayoría de agentes en la lucha contra el *spam*, y que es el de que sólamente reciban publicidad aquellos internautas que lo consientan. Nótese aquí la diferencia: mientras en el último caso se debe dar permiso explícito para recibir publicidad, en la casuística contemplada por la CAN-SPAM se presupone que todo el mundo quiere recibir publicidad mientras no diga lo contrario.
- Otro punto que toca la ley es el que hace referencia a la **forma de conseguir las direcciones de correo** para los envíos. Hasta ahora los *spammers* tenían diferentes caminos para conseguir sus bases de datos de direcciones, como ya explicamos en este trabajo[211]. La ley prohíbe explícitamente la obtención de direcciones de las páginas *web* mediante el uso de programas especiales y el envío masivo de mensajes a servidores de correo electrónico intentando adivinar direcciones válidas a partir de probar combinaciones de letras y números con las extensiones del dominio.
- También se prevé la obligación que el mensaje incluya una dirección física dentro de los Estados Unidos.

Habiendo expuesto los principales puntos de esta ley podemos sacar una serie de conclusiones. Por una parte, no se prohíbe el hecho de recopilar direcciones sin el

[210] Los principales resultados de este estudio se comentaron en los apartados 1.5., "Ejemplos de estafas, prácticas fraudulentas y engañosas que realizan los spammers", 2.1.2. "Naturaleza del *spam*", y 2.4., "Análisis de las cabeceras de los mensajes". En el estudio se analizó el *spam* recibido en 250 direcciones dispuestas en distintos sitios de Internet durante 6 meses.

[211] Consultar el apartado 2.2., "Origen de las direcciones víctimas de spam."

consentimiento del usuario, sino solamente dos formas específicas. De esta forma la pregunta es rápida: ¿como van a saber las autoridades si se ha conseguido una dirección de forma lícita o ilegal?

Por otra parte, se permite el envío de *spam* mediante **opt-out**[212], lo que en la práctica permite a los *spammers* continuar haciendo lo mismo que hasta ahora. En efecto, muchas veces cuando nos damos de baja de una lista de *spam*, al día siguiente empezamos a recibir mensajes de varias más. Esto es así porque muchos *spammers* dan nuestra dirección de baja de forma efectiva, pero la revenden inmediatamente a otras empresas o a sus propias filiales, que a partir de entonces empiezan a usarla con la misma filosofía. En la práctica, esta ley podría venir a legalizar esta situación.

Además, presuponer que un usuario quiere recibir publicidad mientras no indique lo contrario choca frontalmente con lo que piden la mayoría de agentes en la lucha contra el *spam*, y que es el de que solamente reciban publicidad aquellos internautas que lo consientan.

Al margen de la discusión de por qué tiene un usuario que borrarse de una lista en la que nunca dio su consentimiento para que le incluyeran, está el hecho de la tremenda generación de mensajes que conlleva la aceptación de las comunicaciones comerciales mediante opt-out. El método de envío de mensajes de listas de *e-mails* obtenidas a través de opt-out es insostenible, puesto que el número de *e-mails* que se generarían como consecuencia de ello colapsaría el sistema de correo electrónico, si sólo un porcentaje pequeño de empresas en Internet decidieran emplear este método de promoción. Veámoslo con un ejemplo numérico. Si solamente "una décima parte del 1%" de los usuarios de Internet decidieran hacer envíos masivos de *e-mails* a una velocidad moderada con un acceso vía módem y un PC, enviarían un promedio de 100.000 mensajes al día. Entonces todos los usuarios del mundo recibirían 100 mensajes *spam* al día. Si el 1% de los usuarios hiciera ese número de envíos masivos, todos los usuarios recibirían 1000 *spam* al día. Por ello no puede ser razonable permitir el uso del método opt-out para las comunicaciones comerciales por *e-mail*, ya que sería como pedir a la gente que enviara 100 mensajes cada día para darse de baja de una lista. Todo ello que generaría un volumen de mensajes que no sería sostenible por las redes.

3.3.3. Conclusiones.

Tras el análisis de las leyes que legislan actividades relacionadas con el *spam*, en el marco de España, la Unión Europea y de Estados Unidos, se llega a la conclusión de que en muchas ocasiones la mentalidad de los gobiernos en materia de sociedad de la información no siempre es la adecuada para combatir problemas tan importantes como el *spam*. En la Unión Europea, tras la aprobación de la directiva sobre la privacidad y las comunicaciones electrónicas, se insta a todos los países que la componen a prohibir toda forma de comunicación comercial no solicitada y a la forma de envío basado en *opt-in*. Sin embargo se deja un agujero a través del cual cualquier empresa puede enviar las comunicaciones vía correo electrónico que desee siempre que el receptor haya sido cliente suyo. Ello puede redundar en que el usuario se vea saturado de mensajes de compañías de las que es cliente.

Al menos la situación anterior acota el *spam* de alguna manera. Sin embargo la legislación aprobada en Estados Unidos, en mi opinión, lejos de intentar solucionar el

[212] Los términos opt-in y opt-out, fueron adecuadamente explicados en el apartado 3.1.2.1. del bloque II de este trabajo ("Clarificación del significado e implicaciones de los términos opt-in y opt-out"). Por tanto se remite a él para mayor claridad, o al glosario de términos.

problema, lo legaliza. Así legaliza el envío de comunicaciones comerciales bajo una serie de supuestos bastante amplia, basada en opt-out, con lo que se presupone que todos los usuarios desean recibir comunicaciones comerciales o *spam* de cualquiera y de cualesquier tema, salvo pornografía. Esta situación es bastante preocupante en mi opinión dado que un gran porcentaje del *spam* que circula por Internet proviene de Estados Unidos.

Por otra parte e independientemente de cómo esté redactada una ley contra el *spam*, ésta no deja de tener valor únicamente para emisores y receptores que se encuentren en el país de aplicación. Por tanto se trata en mi opinión de una medida para combatir el *spam* que es necesaria pero de efectividad bastante limitada. Es decir, aunque se presuponga que la legislación estuviera bien redactada en un determinado país siempre los *spammers* podrían buscar países sin una legislación adecuada para bombardear a los usuarios. Sí sería más efectiva en cambio si se incluyera la posibilidad de poder extraditar a los *spammers* a los países hacia los que dirigen sus envíos para poder ser juzgados allí, tal y como se contempla en la ley contra el *spam* del Reino Unido.

De todas maneras, y aún cumpliéndose todos los supuestos dichos anteriormente tales que la legislación fuera realmente eficiente, contribuiría a calificar el *spam* como una práctica ilegal pero no representaría un instrumento para acabar realmente con él. En efecto, si nos fijamos en una actividad de mucha mayor gravedad como por ejemplo el tráfico de estupefacientes, se trata de una actividad delictiva en todo el mundo y sin embargo esto no ha contribuido a eliminarla.

4. Medidas de lucha contra el *spam*.

Para combatir de forma eficaz el *spam* es necesario trabajar en diferentes niveles. Según esté en nuestras manos, ya seamos usuarios (receptores del *spam*), creadores de contenidos, o proveedores de servicios de Internet.

Una vez que el *spam* se recibe en un equipo, hay que intentar localizar la fuente originaria, enviar una comunicación al responsable del primer servidor desde donde se realizó el envió el *spam*, filtrarlo de una forma segura para separarlo de los mensajes útiles y finalmente denunciar al emisor de éste en aquellos organismos que investigan o persiguen a los *spammers*.

También tenemos al alcance de nuestra mano una serie de herramientas tecnológicas. Un grupo de ellas se pueden aplicar antes de recibir los mensajes en el servidor destino, mediante un filtrado basado en el análisis de las transacciones SMTP. Por otra parte existe la posibilidad de filtrar los mensajes una vez hayan sido recibidos. Este proceso de filtrado se puede realizar tanto desde la máquina del usuario, como a nivel del servidor del proveedor de servicio.

En este apartado analizaremos estas herramientas, así como otras medidas para combatir el *spam* que proponen los grandes proveedores de Internet, basadas en términos económicos.

4.1. Medidas para combatir el spam impidiendo su recepción[213].

4.1.1. Introducción.

Las medidas de lucha contra el *spam* que se toman para que el mensaje que se detecta como *spam* no llegue a recibirse en el servidor de correo electrónico, implican que la transacción SMTP entre el servidor origen y el destino no finaliza con éxito, y por tanto el mensaje es rechazado. Esta decisión se toma en función del perfil del servidor que pretende enviar el mensaje, o de las características que presenta la cabecera de los mensajes enviados durante el diálogo SMTP. Estas medidas intentan evitar tanto la entrada de *spam* en el dominio, como presionar al origen para que no vuelva a intentarlo, ya que éste recibe todos los mensajes de error que se generan al fallar cada una de las transacciones SMTP necesarias para entregar cada mensaje.

Desde este punto de vista, las medidas que se puedan tomar son más comprometidas para luchar contra el problema del *spam* de raíz. Sin embargo también

[213] Los principales datos que se han utilizado para la elaboración de este apartado han sido tomados de "Luchando contra la publicidad no deseada (o Spam) en el correo" (1 de febrero de 2003), Katja y Guido Socher, LinuxFocus.org, http://www.linuxfocus.org/Castellano/January2003/article279.shtml, de "Evaluación de Alternativas para Reducir el Spam" (mayo 2000), Sanz de las Heras, www.rediris.com y de dos tutoriales: Tutorial sobre Sendmail (en www.seguridad.unam.mx/Tutoriales/Tutoriales /sendmail/sendmail.html) y Tutorial sobre Postfix (2004-02-02) (en http://hal9000.eui.upm.es/halwiki/ Postfix).

son más injustas, puesto que catalogan a un servidor sin dar oportunidad a analizar si su mensaje es *spam* o no.

Para adoptar este tipo de medidas es necesaria la configuración del servidor de correo electrónico, y por tanto éste debe de ser lo suficientemente flexible como para permitirlo. Los dos servidores más utilizados son Sendmail y el de Microsoft, que no permiten mucha flexibilidad en su configuración, sin embargo siempre se puede optar por servidores más flexibles, como Postfix y Exim[214]. Otra alternativa es utilizar un servidor SMTP *proxy* flexiblefrente al servidor de correo electrónico para permitir este tipo de configuraciónes. De esta forma si se quieren implementar en el servidor determinadas medidas de filtrado de mensajes, y éste no lo permite, mediante un servidor *proxy* podríamos conseguirlo sin necesidad de cambiar el servidor de correo.

A continuación se explica el empleo de listas negras y de otros métodos basados en la configuración del servidor de correo electrónico, con el propósito de luchar contra el *spam* antes de su recepción.

4.1.2. Métodos basados en listas negras.

Las listas negras constituyen una medida de lucha contra el *spam* que intenta actuar para que la transacción SMTP no se complete con éxito. De esta forma, el mensaje no llega a entregarse, por lo que no se recibe en el servidor de destino. Se trata de una de las medidas más antiguas y conocidas, y la experiencia demuestra que estas listas bloquean entre el 1% y el 3% del *spam*. Empezaremos exponiendo sus orígenes.

A partir de mediados de los años 90, cuando el *spam* empezó a despertar, el método más habitual de distribuirlo era usando estafetas ajenas *open-relay*[215]. Esto no sólo consumía los recursos de la máquina (disco, CPU y líneas de comunicaciones), sino que evitaban cualquier posible medida legal del país de origen. Muchos servidores empezaron a actualizar su configuración para evitar el uso de sus recursos de forma ilegal.

Simultáneamente, la excesiva cantidad de máquinas *open-relay*, provocó la aparición de múltiples de iniciativas con diferentes técnicas para generar listas o bases de datos que contuvieran un registro con los servidores abiertos que existían. Los incluidos en dichas listas, significaba que eran poco fiables porque con mucha probabilidad enviarían *spam*. La gran labor de las listas negras fue el hecho de obligar a todos los servidores de correo a actualizarse. Por otra parte, dieron a conocer el gran problema del *spam,* constituyéndose como el único mecanismo disponible para combatirlo.

En un primer momento estas bases de datos sólo eran accesibles en local, por lo que cada institución debía tener la suya y no existía coordinación entre ellas. Allá por el 1997 la iniciativa MAPS/RBL ideó un mecanismo de acceso remoto, en concreto vía DNS (Domain Name System), que es el sistema utilizado hoy en día. Se trata de un mecanismo que permite a los servidores de correo electrónico preguntar a dichas bases de datos si la dirección IP (servidor de correo) que se que va a conectar a mi máquina para comenzar una transacción SMTP, está o no está incluida. En caso que estuviera la conexión se cierra, y en caso de que no, se continúa con la transacción. Evidentemente estas listas negras disponían de herramientas para comprobar periódicamente si las

[214] Consultar www.postfix.org y www.exim.org, donde se explican las posibilidades de configuración de dichos servidores para combatir el *spam*.

[215] Consultar el apartado 2.3., "La distribución del *spam*", en el que se analiza y explica el tema de las máquinas abiertas.

máquinas seguían siendo *open-relay* o habían corregido el problema. A partir de este momento, empezaron a aparecer y a venderse muchas iniciativas de listas negras con diferentes criterios.

Así hoy en día, como podemos ver en la tabla siguiente, no sólo existen listas negras con estafetas *open-relays*, sino también con otros criterios diferentes, como que cumplan estrictamente algunos RFCs, listas manuales mantenidas con coordinación internacional, etc. Estas iniciativas obtienen la información de diversas fuentes, entre ellas de las denuncias que introducen los usuarios, y de mecanismos vía *web* para comprobar si una máquina está o no mal configurada. Incluso hay algunas que escanean los puertos SMTP de toda la red en busca de máquinas que puedan ser incluidas en alguna lista.

A continuación se adjunta una tabla con las listas negras más conocidas actualmente. En ella se incluye una columna denominada "Zona DNS", en la que se especifica el DNS que utiliza cada una de ellas. En efecto, las direcciones IP contenidas en las listas se reflejan en una zona inversa del DNS de la organización que lleva la iniciativa, que es consultada en tiempo real por los servidores de correo electrónico que las utilizan en cada transacción SMTP, como hemos explicado.

Tabla 14. Relación simplificada de algunas de las iniciativas de listas negras.

Fuente: www.rediris.com.

Nombre	Zona DNS	Descripción
MAPS/RBL/DUL/RSS (www.mail-abuse.org)	- blackholes.mail-abuse.org - dialups.mail-abuse.org - relays.mail-abuse.org - rbl-plus.mail-abuse.org	Almacena *open-relays*, rangos de marcado telefónico. Los primeros y una de las mejores iniciativas. En 2000 empezó a comercializarse (MAPS RBL+).
ORDB (www.ordb.org)	- relays.ordb.org	Sólo almacena *open-relays*. Actualmente es una de las más sólidas.
ORBZ	- orbz.gst-group.co.uk	Una de las más agresivas. Nació en 1998 y murió en 2001 por problemas jurídicos. Una de las históricas.
FIVETEN (www.five-ten-sg.com/blackhole.php)	- blackholes.five-ten-sg.com	Almacenan diversas fuentes de *spam*: direcciones de grupos de noticias, organizaciones con formularios inseguros, etc.
SPAMHAUS (SBL) (www.spamhaus.org/sbl)	- spamhaus.relays.osirusoft.com	Lista manual de Bloques de IPs de distribuidores masivos de *spam* y/o empresas colaboradoras con el *spam*.
DSBL (www.dsbl.org)	- list.dsbl.org - multihop.dsbl.org	Desde abril 2002. Almacenan *open-relays* que ellos mismos comprueban.
RFC-Ignorant (www.RFC-Ignorans.org)	- dsn.rfc-ignorant.org	Detecta servidores que incumplen RFCs básicos del correo-e: RFC 2821[216], 1123[217], 2142[218], 954[219]. Se haya en continuo crecimiento.
OSIRUS (www.relays.osirusoft.com)	- Relays.osirusoft.com	Almacenan direcciones IP con diferentes criterios: *open-relays*, usuarios, empresas colaboran con el *spam*, servidores de listas que no solicitan confirmación, etc. Actualmente también funciona como agregador de varias listas negras.
Spamcop (www.spamcop.net)	- Bl.spamcop.net	Una de las mejores. Almacena de forma temporal servidores que simplemente han distribuido *spam*.
Spamhaus (www.sbl.spamhaus.org)	- sbl.spamhaus.org	Almacena *open-relays*, *spammers*, etc. Disponen de una amplia red de zonas DNS repartida por Europa y USA.

[216] RFC 2821: Indica que cualquier servidor de correo debe disponer de una dirección de correo tipo <postmaster@...>. *"SMTP servers MUST NOT send notification messages about problems transporting notification messages. One way to prevent loops in error reporting is to specify a null reverse-path MAIL FROM:<>"*.

[217] RFC 1123: Se refiere a MTAs mal configurados que no soportan *"Mail From:*<>", porque lo usan falsamente como medida anti-*spam* (como por ejemplo Terra). *"The syntax shown in RFC-821 for the MAIL FROM: command omits the case of an empty path: "MAIL FROM: <>" (see RFC-821 Page 15). An empty reverse path MUST be supported"*.

[218] RFC 2142: Indica que cualquier servidor de correo debe disponer de una dirección de correo tipo <abuse@..>

[219] RFC954: Básicamente se refiere a direcciones IP que no disponen de datos correctos o desactualizados en las bases de datos *whois*.

Cada una dispone de su propia política de criterios, y contempla unos motivos por los que se ingresa o se sale de ellas. Uno de los aspectos más importantes de una lista negra es la disponibilidad y accesibilidad de un buen soporte rápido de zonas de DNS a ser posible con posibilidad de acceso desde varias partes de mundo. Un acceso lento o una caída de estas zonas supondrían un cuello de botella en la entrada de mensajes en los servidores que las utilizan.

El uso de listas negras como medida para combatir el *spam* tiene dos efectos. Por un lado, llevan a cabo un filtrado que aunque no muy efectivo, elimina y reduce el impacto del *spam*. Se trata de un filtrado que sólo tiene en cuenta la dirección IP del servidor del que proviene el mensaje, y desprecia otras características que podrían ser mucho mejores indicadores de si se trata de un *spam*, como sería el cuerpo y cabecera del mensaje. Por ello deben usarse como complemento de otras técnicas.

Por otro lado, el efecto más beneficioso es que avisan a proveedores y administradores responsables de servidores usados para enviar *spam*, con lo que ayudan a mejorar sus configuraciones y a eliminar a los clientes indeseables que realizan envíos masivos. Además, ejercen una medida de presión para evitar que este tipo de práctica pudiera serles rentable.

Sin embargo las listas negras tienen un importante punto negativo que se deriva de su propia definición, y que hace que mucha gente esté en contra de su uso. Todos los mensajes procedentes de un servidor que esté incluido en la lista negra, serán rechazados. Esto conlleva que podrían ser rechazados *e-mails* correctos procedentes de un servidor de correo electrónico, sin posibilidad de rescatarlos. Además invita a que una organización pueda ser víctima de un *spammer* sin saberlo, y por ello ser incluida en distintas listas negras. Esto le conllevaría una serie de problemas importantes a la hora de utilizar el correo electrónico, aunque fuera con fines lícitos. De esta forma se estaría castigando a inocentes y dejando impune a los verdaderos culpables.

Por este motivo es importante elegir cuidadosamente las listas que se vayan a usar, ya que hay algunas que bloquean rangos completos de direcciones IP simplemente porque un *spammer* utilizó una conexión temporal desde este ISP en algún momento. Desde mi punto de vista, y tras estudiar las características de cada una (ver tabla), el uso de ordb.org sería positivo para eliminar correo procedente de servidores mal administrados (*open-relay*), y de esta forma se evitaría denegar el envío a servidores que podrían no ser utilizados por *spammers*.

4.1.3. Otros métodos basados en el análisis del diálogo SMTP.

Tras describir cómo funcionan las listas negras, en este apartado expondremos algunas técnicas comunes de filtrado basadas también en la configuración del servidor de correo electrónico. En ellas, el servidor comprueba la naturaleza de la cabecera del mensaje que se envía durante el diálogo SMTP, y en función de diferentes características que presenta, puede calificarlo como *spam* y con ello no permitir que la transacción acabe satisfactoriamente (con lo que el mensaje no será recibido).

Algunos servidores presentan muchas más opciones de las que presentamos aquí, pero estas son las más comunes, que suelen estar disponibles cualquier buen servidor. La ventaja de estas comprobaciones es que no usan mucha capacidad de proceso, por lo que generalmente no se necesita actualizar el hardware del servidor para implementarlas. Veamos algunas opciones:

- **8 caracteres no ASCII en la línea del asunto.** Actualmente alrededor del 30% del *spam* se origina en China, Taiwán o en otros países asiáticos. Si se está seguro de

que no se van a recibir mensajes en idiomas orientales (como chino, etc.) entonces se puede rechazar mensajes de correo que tengan 8 caracteres no ASCII en el asunto. Este método es bastante bueno y elimina entre 20-30% de los mensajes *spam* que podrían llegar. Actualmente, esta medida está implementada en la mayoría de los servidores, por lo que no es muy común encontrarse con *spam* que provenga de estos países.

- **Listas con direcciones en el campo *"From:" ("De:")* de *spammers* conocidos**. Esto era efectivo en 1997, pero hoy en día no funcionaría, pues los *spammers* usan direcciones falsas o direcciones de gente inocente[220].
- **Rechazar emisores de dominio desconocido.** Algunos *spammers* usan direcciones que no existen en el campo *"From:"*. No es posible comprobar la dirección completa pero sí se puede conocer a priori la parte del nombre de dominio e investigar si existe a través de un servidor DNS. Esto rechaza aproximadamente entre el 10 y el 15% del *spam*. Esta medida es adecuada porque el usuario normalmente no querría recibir esta clase de mensajes, ya que no podría responderlos aún si no fueran *spam*.
- **Dirección IP que no tiene registro en el DNS.** Se comprueba que la dirección desde la cual se recibe el mensaje pueda ser convertida en un nombre de dominio. Esta medida rechaza bastantes mensajes, sin embargo no es una buena opción porque no comprueba si el administrador del sistema del servidor de correo es bueno, sino si tiene un buen proveedor de red vertical.
  Para conseguir direcciones IP, los proveedores de servicio las compran de sus servidores de red vertical y éstos, compran a servidores de red vertical mayores. Esta cadena normalmente involucra a varios proveedores verticales, por lo que todos tienen que configurar su DNS correctamente para que la cadena de comprobaciones funcione. Si algún intermediario en el proceso comete un error o no quiere configurarlo, entonces no funciona. En resumen, esta medida no aporta mucho con respecto al carácter del servidor de correo individual que se encuentra al final de la cadena, sino más bien del proceso anterior de configuración de direcciones.
- **Requerir comando "HELO".** Cuando dos servidores de correo se comunican entre sí vía SMTP, establecen un diálogo en el que primero envían el comando "HELO", que contiene entre otros datos, el nombre del servidor. Algunos programas de software de *spam* no lo hacen, por lo que filtrar los mensajes que provengan de transacciones de este tipo, rechaza entre 1-5% del *spam*.
- **Requerir comando "HELO" y rechazar servidores desconocidos**. Se trata de tomar el nombre que se obtiene en el comando "HELO", y comprobar en el DNS si es un servidor correctamente registrado. Esta medida funciona en base a que un *spammer* que usa una conexión telefónica temporal, generalmente no configurará un registro DNS válido para ello. Con esta comprobación se bloquea aproximadamente entre el 70 y el 80% del *spam*, pero también puede rechazar muchos mensajes legítimos que provienen de sitios con múltiples servidores de correo en donde un administrador del sistema olvidó de poner los nombres de todos los servidores en el DNS.

Todas estas medidas contribuyen a rechazar un tanto por ciento del *spam* que llega al servidor, sin embargo conllevan que un gran porcentaje de mensajes válidos sean rechazados injustamente, por provenir de un servidor en el que no se han configurado correctamente alguna de las características que se han comentado. En mi

[220] Este aspecto ya se explicó en el apartado 2.4., "Análisis del *spam* mediante las cabeceras de los mensajes".

opinión, sería positivo rechazar por ejemplo mensajes en idiomas orientales, y rechazar mensajes de emisores de dominio desconocido, ya que la mayoría de los *spammers* se inventan este campo.

La ventaja de este tipo de medidas es que no representan un alto consumo de capacidad de proceso en el servidor. Además, aunque se rechacen mensajes válidos, el emisor recibirá un aviso en el que se advierte de que su mensaje no ha sido entregado, por lo éste podrá tomar medidas al respecto. Por este motivo, al igual que los métodos basados en listas negras, representa un tipo de medidas más comprometidas en la lucha contra el *spam*.

4.2. Medidas posteriores a la recepción del mensaje. Filtrado basado en contenidos.

4.2.1. Introducción.

Al hablar de medidas posteriores a la recepción del mensaje, nos referimos con ello a las que se toman después de que el *spam* haya llegado a los servidores o a los buzones, por tanto implican que la transacción SMTP entre el servidor origen y el destino ha concluido con éxito: el mensaje ha sido depositado en la estafeta local.

Funcionan según la filosofía de que si algún patrón de texto aparece a menudo en *spam* pero no en mensajes legítimos, entonces la siguiente vez que se encuentre sería razonable asumir que este *e-mail* probablemente es *spam*. Este tipo de filtrado se puede realizar tanto desde la máquina del usuario, como a nivel del servidor de correo electrónico. Desde este punto de vista, clasificamos las medidas de filtrado de contenidos en dos grupos:

- **Los filtros de contenido instalados en el cliente de correo electrónico** o usuario final, que analizan cadenas de datos que puedan encajar con el contenido de la cabecera o del cuerpo del mensaje tras la recepción de éste en el buzón del usuario. Como resultado de este análisis se decide si el mensaje es *spam* o no. Con los mensajes calificados como *spam* se puede proceder de diversas formas, como borrar directamente el mensaje, o trasladarlo a una carpeta al efecto para que el usuario pueda examinarla en busca de algún mensaje válido.
  Los filtros instalados en el usuario final solucionan algunos de los problemas ocasionados por el *spam*[221], como son reducir los efectos en la gestión del correo por parte de los usuarios: gracias al filtro, el correo no deseado no se ve, y por tanto no molesta. Además, permiten trasladar al destinatario la decisión de configurar sus propios filtros y por tanto de los mensajes que quiere ver y los que no.
  Desde este punto de vista, este tipo de soluciones son bastante eficientes. Sin embargo, no solucionan la recepción del *spam* vía protocolos POP o IMAP, con los problemas de consumo de recursos que conlleva, ya que lo que realmente hacen es ocultar al usuario lo que ya ha llegado a su buzón.
- **Filtros de contenido en el servidor de correo electrónico.** En este caso, el análisis que determina si el mensaje es spam, se realiza en el servidor. Desde aquí también se toma la decisión de la conservación de los mensajes interceptados clasificados como *spam* en directorios de cuarentena para su posterior revisión, o su borrado. Por

[221] Consultar el apartado 1.4., "Efectos del *spam*. Por qué es perjudicial."

tanto, en este caso quien decide los mensajes que son calificados como *spam* es el responsable del servidor.

Los filtros en los servidores solucionan los mismos problemas que los de cliente, pero además evitan que el *spam* llegue al buzón de los usuarios con el correspondiente ahorro de recursos que esto conlleva. Sin embargo, tiene el inconveniente que se deja en manos de los responsables del servicio la creación de las bases de datos de patrones de palabras utilizadas para filtrar el *spam*. De esta forma el usuario no puede de ninguna forma controlar los mensajes que se están filtrando. Para evitar que mensajes válidos no sean entregados, una acción habitual es enviar un mensaje al receptor del *e-mail spam* interceptado, avisándole de lo ocurrido. En él se adjuntan algunos datos del mensaje original, dándole la posibilidad de reclamar en el caso de que lo considerara como válido en un periodo de tiempo de algunos días. Esta medida es positiva porque de esta forma no se tiran mensajes válidos sin consultar al destinatario, y además el usuario no ve el mensaje (sólo los campos "*From*:", "*To*:",...), por lo que el administrador se asegura de que el usuario no abrirá ningún mensaje *spam*. Por otro lado, mengua en gran parte la ventaja del ahorro de recursos que el filtrado en el servidor proporciona, ya que deben enviarse los mensajes de aviso. La elección de cómo llevarlo a cabo dependerá del caso concreto ante el que nos hallemos.

Es importante destacar que el filtrado basado en contenidos (ya sea en el servidor o en el usuario), no soluciona los efectos del *spam* en el ancho de banda de las líneas de la empresa ni en los recursos del servidor, que por el contrario los debe aumentar para poder soportar el consumo que implican los filtros.

Otro punto negativo de estas técnicas es que el servidor de correo que no entrega los mensajes, no advierte de ninguna manera al emisor. Esto significa que un servidor legítimo no recibirá ningún informe de aviso de que su correo se ha rechazado. El mensaje simplemente desaparecerá, por ello no es completamente correcto ya que la recepción de un mensaje realmente depende de las posibilidades del filtro.

Hasta ahora hemos estado diferenciando entre filtros de contenidos instalados en el usuario final y en el servidor. A continuación vamos a exponer las características y modo de funcionamiento concreto de los filtros de contenidos que se están usando actualmente. Para ello realizamos otra clasificación, basada en si el algoritmo de filtrado utiliza reglas estáticas, definidas por el administrador, o se basa en métodos estadísticos. Así, distinguimos filtros estáticos, y filtros bayesianos o adaptativos.

Como veremos, los filtros adaptativos tienen un gran número de ventajas respecto a los filtros estáticos, y en mi opinión serán los más usados conforme su periodo de madurez llegue, y responsables y usuarios perciban a raíz de la experiencia de uso si realmente sus características están por encima. En mi opinión las ventajas de los filtros bayesianos son muchas, por lo que en este trabajo se estudiarán más en profundidad. Veamos ahora cada uno de ellos.

4.2.2. Filtros estáticos basados en reglas.

Se trata de filtros que escanean el contenido de los mensajes que llegan en busca de patrones de palabras o grupos de ellas que indiquen si se trata de un mensaje *spam* o no. Los hemos denominado estáticos porque funcionan comparando los nuevos mensajes con patrones fijos almacenados en una base de datos. El administrador debe introducir y actualizar dichos patrones. Éstos se obtienen de varias maneras:

- A través del análisis de mensajes *spam*, uno mismo puede crearse una base de datos con los patrones más usuales del *spam* que le llega, mediante herramientas disponibles al efecto.
- Si se prefiere externalizar esta tarea, existen proveedores o empresas que se dedican a interceptar *spam,* procesarlo para extraer los patrones más comunes, y generar bases de datos que luego serán descargadas por las empresas clientes para configurar sus filtros, en los servidores o en los usuarios finales.
- También han surgido iniciativas sin ánimo de lucro, en las que los usuarios envían el *spam* que reciben, ofreciéndose como servicio el analizarlo y la tramitación de las denuncias pertinentes. Además el *spam* es reutilizado para la obtención de los patrones que sirven para detectarlo.

Este tipo de filtros de contenidos, instalados en los servidores, son una buena solución corporativa contra el *spam*. Sin embargo la gestión de la base de datos de los patrones usados es compleja, pues depende del idioma y del tipo de *spam* que se reciba, además de requerir su actualización permanente. No obstante, están apareciendo productos de empresas antivirus como TrendMicro (Emanager), McAfee (SpamKiller), etc., que acompañando a los productos para evitar los virus también intentan combatir el *spam*. Si lo pensamos, la filosofía de estos filtros es similar a la de los antivirus, ya que igualmente que se escanean los mensajes en busca de patrones de virus, también se escanean en busca de patrones de contenidos de *spam*. Estas empresas, igual que mantienen y actualizan continuamente sus ficheros de virus, lo están haciendo también con patrones de contenidos de *spam*.

4.2.3. Filtros bayesianos[222].

4.2.3.1. Introducción.

Los filtros convencionales basados en reglas fijas se ha demostrado que son poco eficaces para frenar el *spam,* ya que los *spammers* cambian constantemente sus técnicas y los formatos de sus mensajes para saltarse las barreras que les imponen los servidores. Quienes envían mensajes no solicitados, intentan hacerlos cada vez más parecidos a mensajes legítimos, para no ser eliminados antes de llegar a la bandeja de entrada del usuario.

De modo que los filtros que utilizan como reglas de filtrado la dirección del remitente, el dominio del remitente o alguna palabra del asunto o del cuerpo del mensaje, además de ser muy engorrosos y exigir un trabajo constante de actualización, resultan bastante ineficaces.

Una técnica que mejora considerablemente los resultados en la lucha contra el *spam* son los filtros bayesianos o adaptativos, que pueden ser entrenados por el usuario para que se adapten a los mensajes que él mismo recibe. Uno de los autores que antes planteó esta idea fue Paul Graham, con su ensayo *"A plan for spam"*, en el que plantea aplicar a los filtros *antispam* el Teorema de Bayes de probabilidades combinadas.

En este apartado se expondrán el modo de funcionamiento y las características de este tipo de filtros.

[222] La elaboración de este apartado ha sido posible en gran parte gracias a las ideas de Graham, P. (www.paulgraham.com), junto con el material facilitado por los autores de las conferencias impartidas en "Spamconference 2003" (www.spamconference.com).

4.2.3.2. Definición y algoritmo utilizado en la implementación de un filtro basado en las teorías bayesianas.

El filtrado bayesiano se basa en el principio de que la mayoría de los sucesos están condicionados y que la probabilidad de que ocurra un suceso en el futuro puede ser deducido de las apariciones previas de ese suceso. Esta misma técnica se puede utilizar para clasificar *spam*. Si algún patrón de texto aparece a menudo en *spam* pero no en mensajes legítimos, entonces la siguiente vez que se encuentre el mismo patrón de texto en un nuevo mensaje, sería razonable asumir que este *e-mail* probablemente es *spam*.

Antes de que el correo pueda filtrarse utilizando este método, se necesita generar un antecedente de cada patrón o conjunto de ellos, asignándole un valor de probabilidad de que sea *spam*. Esta probabilidad se basa en cálculos que tienen en cuenta cuán a menudo aparece el patrón en el *spam* frente al correo legítimo, mediante el análisis de los mensajes salientes de los usuarios y del *spam* conocidos. Las palabras y patrones que se analizan se toman tanto del contenido del cuerpo, como de la cabecera.

Teniendo en cuenta lo anterior, el filtro estadístico más simple funciona del siguiente modo. Los usuarios desechan todos los mensajes *spam* en una carpeta separada de los mensajes válidos. En intervalos de tiempo, el programa de filtrado revisa todos los mensajes del usuario, y para cada palabra o muestra, calcula el cociente de las que pertenecen a un mensaje *spam* entre las totales analizadas. Por ejemplo, si una palabra aparece en 200 mensajes *spam* de 1000 analizados y en 3 mensajes válidos de 500 analizados, la probabilidad de que esa palabra pertenezca a un mensaje *spam* es de:

$$P_i = (200/1000) / (3/500 + 200/1000) = 0{,}971.$$

Cada vez que llega un nuevo mensaje, se descompone en palabras, se calculan sus probabilidades de ser *spam* y se toman las *m* palabras con mayores probabilidades, es decir, más cercanas a 0 o a 1 indistintamente (cuyas probabilidades son P_1,..., P_m). De esta manera, la probabilidad de que el mensaje que ha llegado sea *spam* es:

$$P = (P_1*P_2*...*P_m) / ((P_1*P_2*...*P_m) + (1-P_1)*(1-P_2)* ... * (1-P_m)).$$

Normalmente para discernir si el mensaje es *spam* o no, se usa un umbral, es decir, si P (probabilidad de que el mensaje sea *spam*) es mayor que el umbral, el mensaje se califica como *spam*; si P es menor o igual, se califica como mensaje válido. Este umbral suele fijarse alrededor de 0,9, pero este número no es muy relevante porque en la mayor parte de las ocasiones, las probabilidades quedan cercanas a 0 o a 1. En el cálculo de P, los filtros bayesianos usan como máximo $m = 20$ palabras. Si se consideraran más palabras, porque se pensara que algunas de ellas con altas probabilidades de ser *spam* se utilizan también en mensajes legítimos, se comenzarían a incluir patrones que únicamente aumentan el nivel de ruido, elevando el número de mensajes que el filtro considera como *spam*, cuando no lo son.

Este es el caso de algoritmo más sencillo, pero en la actualidad se están usando probabilidades modificadas a partir del Teorema de Bayes para conseguir mejores características de filtrado.

Es importante observar que este análisis se realiza sobre el correo del usuario o la empresa que lo instala en concreto, y por lo tanto es "hecho a medida". Por tanto, la belleza de la filtración bayesiana es que se puede adaptar a cada usuario individual, simplemente aprovechando la información obtenida de clasificar cada *e-mail* recibido. Por ejemplo, una institución financiera podría utilizar una determinada palabra

relacionada con el dinero más veces que un usuario genérico, por lo que obtendría muchos falsos positivos si utiliza una base de datos de reglas *antispam* general. El filtro bayesiano, por otro lado, toma nota del correo saliente válido de la empresa (y reconoce estas palabras relacionadas con el dinero como frecuentemente utilizadas en mensajes legítimos), y por lo tanto tiene mucho mejor ratio de detección de *spam* y mucho menor ratio de falsos positivos.

Después de que el usuario haya clasificado algunos mensajes, el filtro comenzará a hacer esta diferenciación por sí mismo, y generalmente con un nivel muy alto de la exactitud. Si el filtro incurre en una equivocación, el usuario re-clasifica el mensaje, y el filtro aprende de sus errores. Por ello, los filtros bayesianos aumentan su exactitud con tiempo. No se requiere ningún mantenimiento complicado después de que el filtro esté instalado por lo que puede ser fácilmente utilizado por cualquier usuario.

De la explicación anterior se deduce que el filtro bayesiano no es estático, pues se actualiza constantemente en base a los nuevos mensajes *spam* y válidos, aumentando su rendimiento a lo largo del tiempo y adaptándose a los cambios en las tácticas de *spam* y a los cambios de la clase de mensajes escritos por los usuarios.

4.2.3.3. Funcionamiento del filtro en entornos reales.

Parámetros característicos del filtro.

En un entorno de funcionamiento real, podemos medir la calidad del filtro mediante dos indicadores: el porcentaje de mensajes no *spam* calificados como *spam* erróneamente ("tasa de falsos positivos"), y el porcentaje de mensajes *spam* filtrados correctamente ("precisión"). Para este segundo indicador, también puede utilizarse el parámetro "tasa de errores", es decir el porcentaje de mensajes *spam* no detectados, que es equivalente al anterior ("precisión" = 1 – "tasa de errores"). El parámetro más importante desde el punto de vista del usuario real es el porcentaje de falsos positivos. En efecto, si un mensaje *spam* evade el filtro es fácil hacer *click* en el botón de borrar. Sin embargo, si se marca con etiqueta de *spam* a un mensaje normal, el usuario incluso no lo verá, y si era algo importante habrá perdido ese mensaje. Una solución es mirar cada cierto tiempo la carpeta a donde se destina el *spam*, pero esto llega a ser aburrido y una pérdida de tiempo si se reciben muchos mensajes *spam*, además de desperdiciar parte de los beneficios que aporta el filtrado.

Conseguir una precisión cercana al 100% o un número de falsos positivos cercano a 0, es en la práctica es más difícil de lo que podría parecer en un principio. Idealmente se podría conseguir el 0% de errores si marcamos todo como *spam* (umbral ≈ 0), salvo que de esta forma tendríamos que muchos mensajes buenos son marcados como *spam*. Por otra parte podríamos conseguir el 0% de falsos positivos si no marcamos ningún mensaje como *spam* (umbral ≈ 1), sin embargo estaríamos dejando entrar muchos mensajes *spam*.

Por tanto, para conseguir un filtro de alta calidad, y dado que nunca se podrá alcanzar la posición ideal de ambos (ver el gráfico siguiente), hay que intentar conseguir bajas tasas de ambos parámetros llegando a un compromiso, según los valores de estos parámetros que nos interesen. Esto se ilustra en el gráfico siguiente:

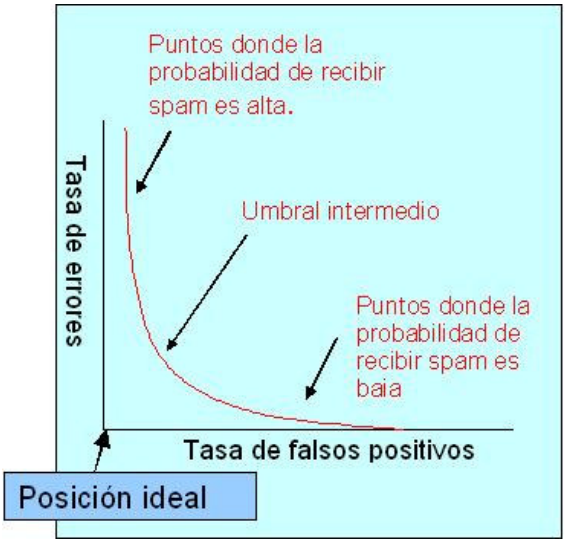

Ilustración 50. Gráfico de probabilidades de un filtro bayesiano. Fuente: www.spamconference.com[223].

Ejemplos de filtros comerciales disponibles. Evaluación del funcionamiento y de las características reales de dos de ellos.

En la actualidad se puede encontrar en el mercado un amplio abanico de filtros basados en métodos estadísticos. Hay dos navegadores que ya incluyen en sí mismos filtros bayesianos: "Mozilla" y "The Opera M2", sin embargo el filtro de éste último tiene una tasa de falsos positivos alta. Para otros gestores de correo, existen una serie de soluciones que pueden instalarse para mejorar las herramientas de filtrado que presentan, que en el caso de Outlook, uno de los más utilizados, son bastante ineficaces. Algunas de las más populares son[224] Spammunition, SpamBayes, Spam Bully, InboxShield, Junk-Out, Outclass, Disruptor OL, y SpamTiger.

En este apartado[225] expodremos los resultados de la utilización de dos de los mejores[226] filtros bayesianos comerciales desde el punto de vista del usuario, según Graham, P.: SpamBayes y POPFile. Para la elaboración de estas conclusiones se llevó a cabo una prueba en la que se contabilizaron el número de mensajes de correo electrónico válidos y *spam* que se recibían, así como la actuación de los dos filtros ante ellos. Las pruebas fueron realizadas bajo las siguientes hipótesis:

- Se usó el protocolo POP3 para la descarga de los mensajes de correo electrónico.

[223] Gráfico traducido a partir del material disponible sobre la conferencia "Spam Filtering. From the Lab to the Real World", Goodman, J., Microsoft Research. Obtenido de www.spamconference.com.

[224] Según Graham, P. (2003), en su artículo "Is there a Bayesian Bayesian filter for Outlook?".

[225] Graham, P. (2003) en su artículo "Winning the War on *spam*: Comparison of Bayesian *spam* filters", del cual se ha extraído parte de la información utilizada para la confección este apartado, quería realizar un análisis comparativo de los filtros bayesianos disponibles en el mercado para el usuario. En nuestro caso, la principal conclusión perseguida al acudir a las conclusiones de este experimento es la de poner de manifiesto cuáles son los parámetros reales y la eficacia de este tipo de filtros.

[226] Las características en las que Graham, P. (2003) se basa para decidir según su opinión cuales son los mejores filtros comerciales de ese momento son que pueda funcionar sobre Windows y Linux, que funcione sobre formas de descargar el correo usando el protocolo POP3, que sea fácil de instalar, de utilizar y sobre todo de realizar las clasificaciones de mensajes.

- Puesto que los filtros bayesianos requieren entrenamiento y su exactitud aumenta con tiempo, la prueba se realizó durante un mes (del 1 de julio al 31 de julio de 2003).
- Tras la segunda semana, la dirección de correo electrónico en evaluación se hizo pública en varias listas de distribución para averiguar cómo se comportaban los filtros ante el *spam* que proviniera de estas fuentes.
- El número máximo y mínimo de mensajes diarios que se recibieron en la dirección de correo electrónico donde se instalaron los filtros durante la prueba, se ha reflejado en la siguiente tabla. En ella se han diferenciado dos periodos: el primer periodo (los 15 primeros días) y el segundo, los 15 últimos días tras la inclusión de la dirección de correo en diferentes listas de distribución. Así, un ejemplo de interpretación de la tabla es la siguiente, para la casilla del primer periodo correspondiente al número de mensajes válidos recibidos: durante los 15 primeros días del transcurso de la prueba se recibieron al día entre 2 y 30 mensajes válidos, de un total diario que osciló entre 30 y 60 mensajes (casilla tercera de la izquierda).

Tabla 15. Resumen del número de mensajes recibidos durante la realización de la prueba.

	1º periodo	**2º periodo**
Máximo-mínimo número de mensajes válidos al día.	30-2	70-20
Máximo-mínimo número de mensajes válidos al día.	50-5	60-40
Máximo-mínimo número total de mensajes al día.	60-30	130-60

Es necesario puntualizar que, asumiendo que la filtración bayesiana uniforme no es siempre perfecta (tasa de falsos positivos siempre distinta de cero), el filtro SpamBayes incorpora una solución que funciona muy bien en la práctica. En lugar de calificar los mensajes entre *spam* o no *spam*, agrega una tercera categoría denominada mensajes "dudosos". El usuario puede configurar cuál es el nivel a partir del cual el mensaje calificado como dudoso se envía a la carpeta de *spam* o a la de no *spam*.

Los resultados de las pruebas realizadas se reflejan en las siguiente gráficas. A la izquierda, se representan los mensajes clasificados erróneamente como *spam* en función del tiempo a partir del inicio de la prueba, para los dos filtros evaluados (SpamBayes y POPfile). En el gráfico de la derecha, podemos apreciar el número de mensajes *spam* no filtrados en función del tiempo, también para ambos filtros.

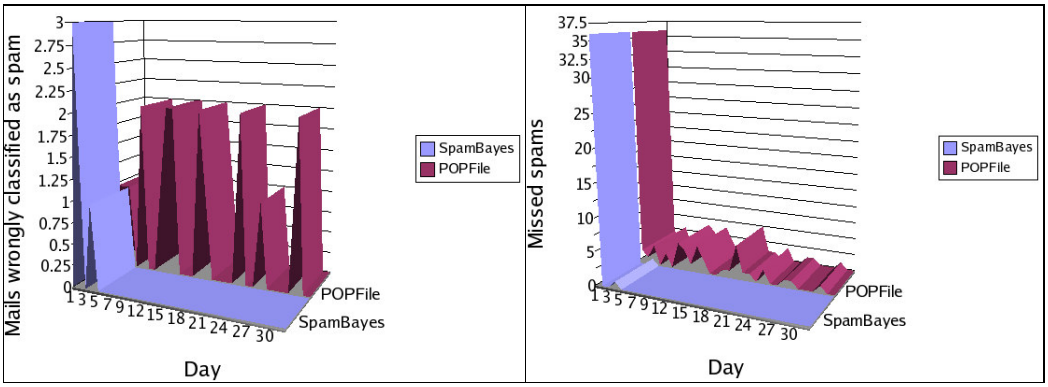

Ilustración 51. Comparativa de los parámetros principales de dos filtros comerciales.

Fuente: www.paulgraham.com.

Se puede apreciar el buen comportamiento de los filtros, ya que tras el periodo de entrenamiento (aproximadamente 5 días en el caso mayor), ambos tienen una tasa de errores y de falsos positivos bastante baja. Sin embargo, aunque PopFile trabaja bastante bien, se puede apreciar como la tasa de falsos positivos es oscilante a lo largo del tiempo. Esta característica podría considerarse grave, pues incluso un solo *e-mail* incorrectamente clasificado como *spam* es demasiado, ya que nunca se está seguro de la importancia que tenía dicho mensaje. El filtro SpamBayes es bastante mejor en este aspecto, puesto que no dio ningún falso positivo tras su periodo de entrenamiento. Para el parámetro errores, de nuevo se puede apreciar que los resultados del SpamBayes son superiores.

El porqué de esta diferencia es el hecho de poseer una tercera clasificación de los mensajes como "dudosos". Sin embargo esto hace que la comparación no sea totalmente justa, puesto que sus principios de funcionamiento son distintos. Para realizar una comparación más real, en el siguiente gráfico se han incluido los mensajes clasificados por el filtro SpamBayes como "dudosos".

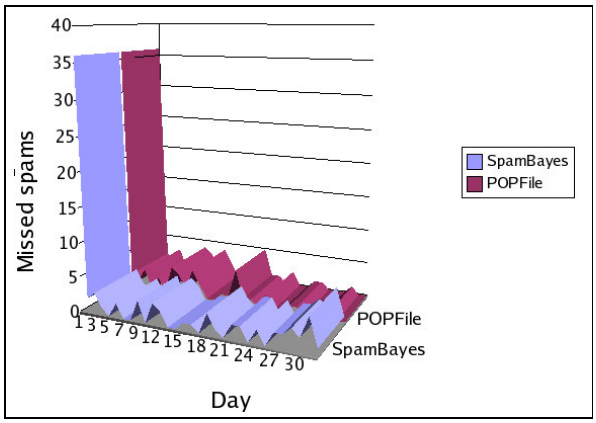

Ilustración 52. Comparación real entre los filtros SpamBayes y POPFile.

Fuente: www.paulgraham.com.

En este gráfico podemos ver que realmente el filtrado bayesiano básico que incorporan ambos filtros es más o menos igual si consideramos que éste califica todos mensajes dudosos como correo válido para evitar falsos positivos.

La principal conclusión de la exposición de los resultados de este experimento es que en total, con ambos filtros se consiguieron tasas de aciertos de 97.75% con pocos falsos positivos, lo cual se considera bastante bueno. Sin embargo, pruebas realizadas en cuentas de correo de otros usuarios demostraron que se pueden conseguir tasas del 99%.

Análisis del tipo de palabras que utiliza un filtro bayesiano en su decisión estadística.

Como hemos mencionado anteriormente, para el cálculo de la probabilidad de que un mensaje sea *spam*, se tienen en cuenta todas las características del mensaje, tanto el contenido del cuerpo, como el de la cabecera. De ella se pueden obtener muchos datos interesantes, tales como el remitente, el origen del mensaje, u otros en apariencia menos importantes como la hora en la que se realizó el envío, que pueden servir de gran

ayuda en la clasificación del mensaje. Por ejemplo, un mensaje que se haya enviado en horas de madrugada, es más probable que sea *spam*[227].

A continuación, se adjunta un ejemplo del tipo de palabras del cuerpo del mensaje que un filtro bayesiano califica con alta probabilidad de ser *spam*, que han sido tomadas de un usuario concreto[228]. Después de cada palabra, aparece entre paréntesis la probabilidad que le corresponde (a mayor probabilidad, más posibilidades de que el mensaje que la contenga sea *spam*). Como se puede deducir de la explicación anterior, estas palabras no son estándar ni iguales para todos los usuarios, sino que el propio filtro las elige según los mensajes que han llegado al buzón de dicho usuario.

Palabras que presentan grandes probabilidades de ser *spam*:

- *Money (2356/48).*
- *Sex (1989/34).*
- Pronombres en segunda persona *(you (1560/1034), your (1465/367), our (1118/125).*
- Palabras que indican urgencia u obligación *(must (201/116), important(125/24), critical (13/5), urgent (32/1))*
- Palabras que expresan tiempo*, (January (40/24), today (186/23) (not yesterday (1/7)), week (68/27), month (186/16), year (129/43)).* Esto sucede a pesar de que en el cuerpo de los mensajes legítimos a menudo aparecen este tipo de palabras.
- Palabras relacionadas con una respuesta por parte del destinatario *(reply (215/17), call (235/90), email (909/143), telephone (76/8), letter (100/9), Requirements (require (52/25), obligation (106/2), must (201/116)).*
- Palabras neutras: *get (710/390), are (1065/635), make (383/229), trust (40/24), this (1299/809).*

Ilustración 53. Ejemplos de palabras calificadas con altas probabilidades de pertenecer a mensajes spam. Fuente: www.jerf.org.

[227] Consultar el apartado 2.1., "Análisis de la situación del *spam* en cifras. Estudios y estadísticas".

[228] Las palabras que adjuntamos a continuación han sido tomadas de las pruebas efectuadas por Bowers, J. (www.jerf.org) con un filtro bayesiano. Se trata de un usuario de lengua inglesa, por lo que las palabras corresponden al inglés.

Palabras que presentan pequeñas probabilidades de ser *spam*:

- Las contracciones inglesas. *I'm (46/462), we'd (1/14), I'll (24/126). Excepciones: won't (99/56), you'd (69/33).*
- Pronombres en primera persona *(mine (4/27), I'd (14/150), I'm (46/462)).*
- Palabras que expresan sentimientos negativos *(hate (5/42), kill (2/46), sad (1/7), evil (1/27)).*
- Lenguaje coloquial o *slang* en inglés (acrónimos coloquiales en la lengua inglesa como *YMMV, smileys like (1/84), (2/104)).* También otras palabras propias del mundo en que se mueve el usuario.
- Palabras neutras: *but (314/887), should (140/261), they (289/495), that (921/1260).*

Copyright 1999-2003 Jeremy Bowers. www.jerf.org.

Ilustración 54. Ejemplos de palabras calificadas con bajas probabilidades de pertenecer a mensajes *spam*. Fuente: www.jerf.org.

Aunque el ejemplo ha sido tomado de un usuario concreto y de habla inglesa, las palabras que aparecen con altas y bajas probabilidades, pueden corresponderse con las que estarían definidas para un usuario más o menos estándar. Así, si nos fijamos en características de los mensajes *spam*, llegamos a la conclusión de que palabras como dinero, sexo, palabras que expresan urgencia u obligación y palabras relacionadas con una respuesta por parte del destinatario, es fácil encontrárselas en este tipo de mensajes. Por otra parte, expresiones muy coloquiales y estilo de redacción en primera persona son características que todos usamos al escribir y recibir nuestros mensajes. Además, la mayoría del *spam* que se recibe está en inglés, con lo que probablemente muchas palabras con alta probabilidad de *spam* de nuestro filtro estarían en esta lengua.

Sin embargo, con este ejemplo no se quiere indicar que las características de los mensajes válidos y *spam* son iguales en todos los usuarios, todo lo contrario. Por ello, la ventaja más importante de los filtros basados en métodos estadísticos es su adaptación dinámica al usuario y al *spam* de cada momento.

4.2.3.4. Ventajas del filtrado bayesiano frente a filtrados estáticos. Adaptación a la evolución del *spam*.

Como hemos venido explicando hasta el momento, el filtrado bayesiano tiene una serie de ventajas respecto al filtrado basado en análisis de palabras clave, o en listas negras. En este apartado se pretende resumir y analizar dichas ventajas. Entre las más importantes se encuentra como ya hemos indicado, el hecho de que este tipo de filtros puede adaptarse al correo de cada usuario concreto, pero también a los mensajes indeseados que lleguen. En este ámbito, se analizarán una serie de técnicas que han sido usadas por los *spammers* con la intención de burlar los filtros y como éstos se han adaptado a los nuevos formatos de *spam*. Veamos en primer lugar las ventajas que representa el filtrado bayesiano.

1. El método bayesiano tiene en cuenta la totalidad del mensaje. En efecto, reconoce palabras clave que identifican el *spam*, pero también reconoce palabras que

denotan que se trata de mensaje válido. Por ejemplo, no todo el correo que contiene las palabras *"free"* y *"cash"* es *spam*. El método bayesiano encontraría relevantes las palabras *"cash"* y *"free"* pero también reconocería el nombre del contacto de negocio que envió el mensaje, y de ese modo lo clasificaría como legítimo, por ejemplo. En otras palabras, el filtrado bayesiano es una estrategia más inteligente que otros métodos porque examina todos los aspectos de un mensaje, en oposición al análisis de palabras clave que clasifican un mensaje como *spam* en base a un solo conjunto de palabras fijo.

2. Un filtro bayesiano están constantemente auto-adaptándose. Mediante el aprendizaje continuo a través de los nuevos mensajes (*spam* y válidos), el filtro bayesiano evoluciona y se adapta a ellos. Así, si surgen nuevas técnicas *spam*, el filtro aprenderá a reconocer el nuevo tipo de mensajes no deseados. Por otro lado, también se reconfigura ante los posibles cambios que se den en el correo válido que llega al usuario. De este modo, si éste comenzara a recibir mensajes de correo electrónico deseado de una determinada lista de distribución relacionada con un tema que pueda asociarse a mensajes *spam*, y del que antes nunca se había recibido ningún mensaje, el filtro se adaptará y permitirá la entrada de este nuevo tipo de mensajes, pero no de mensajes *spam*.

3. La técnica bayesiana es sensible al usuario. Para tener éxito y hacer que se entreguen sus mensajes, los *spammers* tienen que enviar correo que no sea atrapado por los filtros personalizados de la víctima. Como el método bayesiano tiene en cuenta el perfil de correo del usuario, detecta el *spam* con mayor facilidad, pues los *spammers* necesitarían saber el perfil de correo de dicho usuario para ser capaces de superarlo. Dado que el *spam* tiene su propio vocabulario y carácter, el filtro bayesiano puede atraparlo con facilidad. Sin embargo, no es sencillo para los *spammers* cambiar sus argumentos de venta para tener en cuenta el perfil de correo del usuario, pues una de las principales características del *spam* es que es masivo y no personalizado.

4. El método bayesiano funciona adaptándose a cualquier lengua y es internacional. Un filtro *antispam* bayesiano al ser adaptable, puede utilizarse con cualquier idioma necesario, siempre que éste utilice como separadores de palabras el carácter espacio (" "). La mayoría de las listas de palabras clave indicadoras de *spam* disponibles para filtros estáticos, sólo lo están en inglés y son por lo tanto mucho menos útiles en regiones de habla no inglesa. El filtro bayesiano también tiene en cuenta ciertas desviaciones del lenguaje o los diversos usos de ciertas palabras en áreas diferentes, incluso si se habla el mismo idioma. Esta inteligencia lo habilita como un filtro más efectivo.

5. Un filtro bayesiano es más difícil de burlar que un filtro de palabras. Para intentar demostrar e ilustrar esta ventaja, a continuación vamos a enumerar las posibles diversas técnicas que he observado que los *spammers* utilizan o podrían utilizar con la intención de burlar el filtro, y cómo éste "aprendería" a detectarlas.

- Un *spammer* avanzado que quiera engañar a un filtro bayesiano podría **elegir las palabras** de su mensaje de tal forma que utilizara menos palabras con alta probabilidad de pertenecer a un mensaje *spam* (es decir, palabras que habitualmente indican *spam* como *free*, *Viagra*, etc.), o más palabras que generalmente indican correo válido (como un nombre de contacto válido, los apodos de los amigos o términos que se usan normalmente en el ámbito laboral de cada usuario). Haciendo lo último es imposible porque el *spammer* tendría que conocer el perfil de correo de cada destinatario, y esto es imposible puesto que todos son diferentes. Además, si los *spammers* intentaran burlar el filtro mediante palabras que normalmente se califican como buenas, eso no sería suficiente porque en un mensaje *spam* típico, un montón de palabras con alta probabilidad se encuentran ya en la cabecera. Estas

últimas irían aumentando la probabilidad de calificar el mensaje como *spam*. Por otro lado, utilizando palabras neutras, por ejemplo la palabra *"public"*, no funcionaría ya que éstas son dejadas de lado en el análisis final (sólo se utilizan las "m" con probabilidades más cercanas a 0 o a 1). Por tanto, la técnica de utilizar palabras "más apropiadas" no engañaría al filtro.

- Incluir en los mensajes palabras que típicamente indican que se trata de un mensaje *spam* pero **intentando encubrirlas**. Por ejemplo, utilizando *"f-r-e-e"* en lugar de *"free"*. Otro ejemplo sería utilizar la palabra *"5ex"* en lugar de *"Sex"*. También podrían utilizar como separadores hipervínculos html, espacios en blanco y otros caracteres, por ejemplo *"fr ee"* en lugar de *"free", "frèé"* o *"fr.ee"* en lugar de *"free"*). Pero esto sólo incrementará la probabilidad de que el mensaje sea *spam*, ya que un usuario legítimo raramente escribirá la palabra *"free"* como *"f-r-e-e"*. En este caso, el filtro bayesiano advierte automáticamente estas palabras que nunca se usarían en mensajes válidos por regla general, por lo que sería capaz de adaptarse para atrapar este tipo de *spam*.
- Otra táctica es enviar **mensajes que** no **contengan** texto, **sólo imágenes**. Los mensajes con imágenes tampoco engañarían al filtro bayesiano por varias razones. Para empezar, las cabeceras que sugieren que el mensaje es *spam* nunca pueden omitirse. Además el filtro comprueba tanto texto como el código HTML. En el cuerpo del mensaje probablemente habrá un *link* a la imagen, y ambos contendrán una dirección URL, la cual probablemente tenga una alta probabilidad de ser *spam*. Con el hipervínculo, la imagen tendrá alguna clase de nombre, y este está normalmente lejos de ser aleatorio. Por tanto, cualquier imagen que contenga el *spam* tendrá asociadas en el cuerpo del mensaje o en el código HTML algunas palabras, que servirán para catalogar el mensaje como *spam*.
- Añadir al mensaje **palabras invisibles**, tratando de confundir al filtro: "si el usuario no puede verlas, el filtro tampoco". Ejemplos de esto, puede ser añadir texto en blanco sobre fondo blanco, cabeceras de los mensajes que incluyan las palabras deseadas, o incluyendo palabras aleatorias antes del código HTML. Sin embargo el filtro es capaz de leer el código HTML de los mensajes y sus cabeceras, por lo que estas técnicas no funcionarían.
- Insertar una falsa **etiqueta HTML** que contenga un largo texto, por ejemplo de una noticia. Si observamos el código de un mensaje, las etiquetas van entre los caracteres "<" y ">". Los bloques de texto largo en el código del mensaje son omitidos por los servidores HTML, por tanto aparecerán como etiquetas no válidas. Además, la etiqueta necesita definirse en el código del mensaje, por lo que de ninguna manera pasará desapercibida para el filtro.
- Otra forma de intentar burlar el filtro podría ser que el contenido del mensaje solamente fuera un hipervínculo al sitio a promocionar, estando **la URL del hipervínculo codificada en decimal**, hexadecimal u octal. Este tipo de tácticas obligarían a que el filtro decodificara el texto HTML. Algunos filtros ya reconocen estas variantes y traducen las URLs a su forma canónica.
- Reemplazar el texto del *spam* por **código *Javascript*** tal que se ejecutara al abrir el mensaje. Este sería un buen truco, a no ser porque el usuario rara vez codifica sus mensajes en *Javascript*. Sin embargo, los filtros actuales no presentan buenas soluciones ante esta táctica.

Se ha puesto de manifiesto la imaginación de los *spammers* y cómo un filtro basado en métodos estadísticos podría seguir funcionando correctamente ante ellas. Como conclusión se deduce que el uso masivo de estos filtros podría ser el fin de mensajes que anuncian temas muy concretos tales como los que anuncian hipotecas,

pornografía, etc., pues es muy difícil anunciar hipotecas sin usar ninguna de las palabras como "préstamo", "interés", "hipoteca", etc., que por otra parte son muy raramente utilizadas en usuarios comunes.

4.2.3.5. Aplicación del filtrado bayesiano en servidores.

Usar filtrado bayesiano en servidores de *e-mail* es algo más complejo que en los buzones de compañías o de usuarios individuales, puesto que debe de haber una manera para que los usuarios individualmente entrenen el filtro, ya que no es fácil establecer un perfil correcto de todos los usuarios de un proveedor. Varios ejemplos de filtros bayesianos que trabajan en servidores son SpamProbe, Razor y Bogofilter.

Es interesante comentar la filosofía de uso de **Razor**[229]. Se trata de un sistema de detección y seguimiento de mensajes *spam*, distribuido y colaborativo. Su funcionamiento está basado en que el *spam* típicamente opera enviando idénticos mensajes a cientos de personas. El sistema de Razor permite que la primera persona que reciba el *spam*, lo añada a la base de datos, para que el resto de las personas bloqueen ese mensaje en concreto. Su algoritmo calcula sumas de verificación de estos mensajes *spam* conocidos, y también se almacena en la base de datos distribuida. Si se recibe un mensaje nuevo, se computa la suma de verificación y se compara con las sumas de verificación en la base de datos central. Si coinciden, se rechaza el mensaje. Razor basa su funcionamiento también en cuentas especiales de correo distribuidas en Internet con el único propósito de ingresar en las listas de direcciones de todos los *spammers*. Estas cuentas sólo captan *spam* y no correo normal y contribuyen a actualizar la base de datos. Los clientes también pueden enviar mensajes a Razor para que el sistema los incluya. La gran ventaja de este sistema es que existe una alta probabilidad de que los mensajes ya sean conocidos como *spam* antes de que lleguen al buzón de correo. El sistema filtra alrededor del 80% del *spam* con la característica de que no tiene ningún otro proceso o técnica de filtrado, por lo que detecta muy pocos falsos positivos.

Otra alternativa para los filtros estadísticos en servidores es la utilización de filtros basados en métodos heurísticos, que proporcionan mejores características en este tipo de entornos. En efecto, según la empresa MessageLabs[230], la tasa de *spam* filtrado mediante técnicas bayesianas, que en usuarios individuales llega hasta el 99%, en servidores desciende entre el 80 y el 95%. Sin embargo, los filtros basados en métodos heurísticos, proporcionan en media un porcentaje de aciertos en torno al 95%.

4.3. Comparativa tras el análisis de las medidas contra el spam.

En el apartado 4.1 ("Medidas para combatir el *spam* impidiendo su recepción"), comentamos que se puede realizar un primer filtrado de mensajes configurando el servidor de correo electrónico, para que rechace unas determinadas transacciones SMTP que presenten evidencias de que sean de *spammers*. Estas medidas consiguen evitar un porcentaje de *spam* pequeño, pero tienen la gran y exclusiva ventaja de que avisan al servidor emisor de que su mensaje no será recibido. Además, consumen muy pocos

[229] Consultar http://razor.sf.net.

[230] Documentación de la conferencia "Internet Level Spam Detection and SpamAssassin 2.50", Sergeant, M. (Senior Anti-Spam Technologist), MessageLabs, obtenido de www.spamconference.com.

recursos del servidor receptor, ni en términos de procesado de algoritmos de filtrado (que a veces resultan muy pesados), ni de ancho de banda en redes.

Una de las medidas basadas en el análisis de las transacciones SMTP que presentan más controversia, son las basadas en listas negras, que consisten en el rechazo de las transacciones SMTP (y por tanto de los mensajes) que provengan de determinadas direcciones IP. Los defensores de las listas negras alegan que son una medida justa, puesto que ejercen presión al proveedor que aloja a *spammers*, haciendo que mejore su configuración (en el caso de que sus servidores estén abiertos), o para evitar que este tipo de práctica pudiera serles rentable y eliminen a los clientes indeseables que usan técnicas de *spam*. Sin embargo, presentan una serie de inconvenientes:

- El porcentaje que se recibe de *spam* de un grupo de remitentes concreto, por muy grande que sea, representará un porcentaje pequeño del *spam* total que recibimos, ya que los *spammers* cambian dinámicamente de dirección.
- El hecho de incluir un servidor en una lista negra hace que no se reciba ningún mensaje que provenga de él, sea *spam* o no. De este modo pagan mensajes justos por pecadores.

Por otra parte, tras el análisis realizado de las medidas de filtrado basadas en contenidos (apartado 4.2.), se puede concluir señalando una serie de ventajas y desventajas que conlleva su utilización, en comparación con las medidas tomadas para impedir la recepción del mensaje (apartado 4.1.). En primer lugar, exponemos los aspectos positivos:

- Se disminuye notablemente el *spam* de los buzones, al ser enviado a una carpeta separada del correo válido. Con esto se consigue que la molestia que sufre el usuario al tener que buscar los mensajes válidos se vea reducida.
- Si los filtros eliminan algún mensaje correcto, siempre es posible buscarlo en las carpetas de correo no deseado.
- En los filtros en el receptor final, la decisión de lo que es *spam* recae en el usuario que lo sufre, ya que es él quien define los filtros. Por otra parte en los filtros de servidor, la decisión de lo que es *spam* está definida en la "política institucional para el uso del servicio de correo electrónico"[231], por tanto la responsabilidad de decidir qué es *spam* recae en los administradores de la misma.
- Usar un filtrado basado en contenidos puede evitar el abuso por considerar a un inocente en una lista negra, que a veces puede hacer más daño que el mismo problema del *spam*. Este tema es preocupante puesto que a menudo los *spammers* utilizan servidores de víctimas inocentes.

Por otra parte, la utilización de filtros de calidad basados en contenidos puede poner fin a la ficción que muchas veces se esconde tras el *opt-in*. En efecto, el *opt-in* que dicen practicar algunas compañías no es sino una forma de enmascarar el *spam*. Una de las empresas que presume poseer mayor número de direcciones obtenidas mediante *opt-in*, tiene alrededor de 60 millones de direcciones correctas, y casi todas de usuarios domésticos. 60 millones de usuarios de Internet representan alrededor de la mitad de los usuarios de Internet de EEUU. Sin embargo si se preguntara a estos usuarios si recuerdan haber solicitado esta publicidad, probablemente no lo recordarán. Este ejemplo ilustra que existe mucho engaño en este ámbito. Los *spammers* que se esconden tras este método de envío de publicidad no intentan esconder su identidad ni el tema que anuncian, es decir, sus mensajes indican abiertamente de dónde proceden y de

[231] Consultar el apartado 3.2.3., "Consejos a los PSI y los administradores de servidores de correo electrónico.".

qué se trata. Por ello estos mensajes pueden ser fácilmente capturados por los filtros de contenidos.

Por otra parte, el filtrado de mensajes basado en contenidos como medida para combatir el *spam* tiene una serie de aspectos negativos:

- El *spam* es encaminado por las líneas de comunicaciones y procesado como mínimo por las estafetas de correo electrónico, por tanto no elimina los problemas del consumo de recursos.
- Los mensajes deseados que se descartan pueden ser de gran importancia para el usuario, y sin embargo ni emisor ni receptor son avisados. Esta característica elimina la ventaja de que el correo electrónico es seguro, por lo que los emisores deberían preocuparse de comprobar que sus mensajes han sido leídos por los destinatarios. En contraposición, en el caso de uso de listas negras, se notifica al remitente que su mensaje no ha sido entregado, por lo que éste puede tomar medidas.
- No se trata de técnicas que tengan efectos en la erradicación del *spam*, desde el punto de vista de que:
    - Ni emisores ni proveedores responsables reciben ningún tipo de información: no avisan al emisor o proveedor de servicios afectado de que se está llevando a cabo una actividad incorrecta, con lo que éstos pueden desconocerlo y ser también víctimas de los *spammers*.
    - Lo que realmente se hace con los mensajes es esconderlos en lugares habilitados al efecto (carpetas en el usuario final, o en directorios en el caso de filtros en el servidor), pero realmente los mensajes son recibidos.

Presentadas las ventajas y desventajas de ambas filosofías de filtrado, a continuación se resumen en la siguiente tabla sus características numéricamente, a modo de tabla comparativa[232].

Tabla 16. Comparativa de las características de los distintos filtros.

Fuente: MessageLabs, www.spamconference.com.

	Listas negras (DNS)	**Análisis del diálogo SMTP**	**Filtros de palabras**	**Métodos heurísticos**	**Métodos estadísticos**
Precisión	0 - 60%	hasta 30%	80%	95%	99%+
Falsos positivos	10%	-	2%	0.5%	0.1%

Los resultados que hemos presentado acerca de las tasas de filtrado que pueden llegar a conseguirse con técnicas estadísticas, podrían despertar esperanza en el hecho de que el *spam* puede llegar a controlarse, sin embargo los límites del *spam* son insospechados y habrá que ver qué nos depara el futuro.

[232] "Filters vs. black list" (septiembre de 2002), Graham, P., www.paulgraham.com y documentación de la conferencia "Internet Level Spam Detection and SpamAssassin 2.50", Sergeant, M. (Senior Anti-Spam Technologist), MessageLabs, obtenido de www.spamconference.com.

4.4. Hacia dónde llevan las nuevas medidas contra el spam. Opinión de los grandes proveedores[233].

Según algunos grandes proveedores de Internet, que son los mayores afectados por el *spam* desde el punto de vista económico, los filtros *antispam* no ofrecen una solución decisiva a su problema, por lo que intentan buscar nuevas herramientas y tácticas. Bill Gates, presidente del gigante del software y de Internet Microsoft, lidera un movimiento que está empezando a tomar fuerza, y que apuesta por combatir el *spam* haciendo que los *spammers* paguen los recursos que utilizan.

La razón por la que el *spam* representa hoy más de la mitad del tráfico en Internet, es porque actualmente, el emisor (*spammer*) paga un precio marginal cercano a cero por realizar sus envíos. Para los *spammers,* esta situación representa una estrategia de beneficio seguro: "envía tanto como puedas, porque incluso un si un usuario de cada millón se transforma en cliente, es rentable".

Una solución obvia podría ser por tanto cobrar por el envío de estos mensajes. En el World Economic Forum celebrado en Davos (Suiza) en enero de 2004, Bill Gates de Microsoft defendió que la tecnología de filtrado junto con esquemas de pago podrían frenar y eliminar el *spam* en dos años. Otras compañías también opinan que algún sistema que haga pagar a los *spammers* por sus envíos, podría contribuir si no a eliminar el *spam*, sí a reducir las pérdidas que deben afrontar los proveedores de servicio. Veamos algunas ideas de varias empresas que se basan en este planteamiento:

- Según Richard Gingras, director de la compañía **Goodmail Systems**, su idea es crear una especie de "sellos electrónicos", de forma que los *spammers* que deseen que sus envíos masivos sean entregados, asuman un coste por ello.
  Por ejemplo, Amazon afirma que compraría un millón de "sellos de *e-mail*" a 0,01 dólares cada uno, si sus mensajes de confirmación automática de pedidos que le reportan una parte importante de sus ventas, no fueran filtrados como *spam* por error. Ello redundaría en un beneficio de 10.000 dólares para el proveedor de servicio. Goodmail, como compañía encargada de la gestión de este sistema, pondría los sellos a los mensajes de Amazon como cabeceras encriptadas, y enviaría la clave para desencriptarlos al ISP. El ISP en este caso podría identificar los mensajes de Amazon, y entregarlos a los buzones de los consumidores.
  Bajo el sistema que propone Goodmail, los *spammers* serían libres de comprar estos sellos, al igual que los que realizan buzoneo a través del sistema de correos convencional. Sin embargo, esto introduciría en sus economías un gasto extra y justo. En esta situación los mensajes de los *spammers* que no compraran los sellos, serían ilegítimos y los proveedores podrían filtrarlos con mayor facilidad, con lo que se reduciría el *spam*, incluso si el sistema es adoptado sólo parcialmente.
  Sin embargo, según otras opiniones, este sistema podría ser inviable al tener que procesar millones de paquetes de datos en los que se fragmenta cada mensaje, tratando de separar los que deben cobrarse.
- Un método adicional, propuesto por la compañía **IronPort System**, no carga en los emisores todo el coste de todos los mensajes, sino sólo los que hayan provocado una queja de los receptores. Esta compañía ha venido ofreciendo desde hace poco más de un año, un servicio a emisores masivos de mensajes, como son el caso de las compañías que envían boletines electrónicos. Se trata de un contrato de tal forma

[233] Parte de las ideas utilizadas en la elaboración de este apartado han sido tomadas del artículo "Make'em pay" (12 de febrero de 2004), www.economist.com y "¡Guerra al Spam!" (5 de febrero de 2004), Guillem Alsina, www.diariored.com.

que, a cambio de previo pago, entrega sus mensajes a los receptores. Los emisores deberán abonar además un pago extra si los emisores se quejan del mensaje. La idea es disponer de una especie de lista blanca que eventualmente crece con los emisores que sean calificados como honestos por los usuarios, y en otro caso, son incluidos en listas negras.

- Alguna gente quiere ir más lejos. Balachander Krishnamurthy, de **AT&T Labs**, proponía un sistema en el cual el ISP establecería un consorcio (similar al que establecen los bancos con Visa), en el que el proveedor actuaría como modelador entre el emisor y los usuarios. Se daría a los emisores que establecieran el contrato un número de créditos limitados. Cada vez que un receptor declarara un mensaje como no solicitado al modelador, se cobraría al emisor de ese mensaje 1 dólar, por ejemplo. Una vez agotado el crédito asignado (por ejemplo 200 dólares), el modelador suspendería el servicio a ese emisor.

Según esta corriente de opiniones, estos esquemas también servirían para intentar solucionar otro gran problema: el envío de *spam* mediante la propagación de virus, como el Sobig y el MyDoom[234], que convierten a los ordenadores de usuarios inocentes en máquinas de enviar *spam*. En el último sistema descrito, el crédito limitado de los usuarios infectados por un virus de este tipo, se agotaría en pocos segundos, con lo que pararía de propagarse. El PSI podría detectar que en estos casos los usuarios son víctimas, y devolverles el servicio una vez solucionado el problema.

Sin embargo en mi opinión, estos sistemas basados en que la queja del usuario revierta en un coste para el *spammer*, ocasionarían que aunque los problemas económicos de los proveedores se verían atenuados, el problema de los usuarios se incrementaría notablemente. En efecto, en esta situación les llegarían a su buzón muchísimos mensajes más que en la situación actual, puesto que éstos llegarían con el visto bueno del proveedor y no se filtrarían. Además el usuario debería emplear mucho más tiempo en abrir los mensajes, decidir si son o no ofensivos, y efectuar una queja. De hecho, la gran mayoría de los usuarios no se quejaría.

En conclusión, todos estos esquemas tienen el denominador común de que si el proveedor detecta que un mensaje es "*spam* legítimo", lo entrega. Por tanto estos esquemas sólo están beneficiando a la gran empresa que realiza el *spam* y que le es rentable pagar por él y al mismo proveedor, que consigue ingresos extra. Pero en ningún caso se beneficia al usuario, que en esta situación se vería inundado de *spam*.

4.5. Cómo se debe actuar ante el spam recibido: quejas y denuncias[235].

En este apartado se aconseja qué debe hacerse cuando recibimos *spam*, con el fin de contribuir a la lucha para combatir el problema. Siempre podemos llevar a cabo alguna acción desde nuestra posición, ya seamos usuarios, o administradores de correo electrónico en alguna organización. Es importante destacar que todas las medidas que se tomen para combatirlo contribuirán de forma importante a luchar contra el *spam*.

[234] Consultar el apartado 3.2.3.1. del bloque II de este trabajo, "Mediante el uso de códigos maliciosos."

[235] Algunas de las pautas a seguir recomendadas en este apartado, han sido tomadas de las recomendaciones de la AUI (Asociación de Usuarios de Internet, www.aui.es), la AI (Asociación de Internautas, www.internautas.org), y de la organización RedIris (www.rediris.es).

4.5.1. Desde el punto de vista del usuario.

Las entidades de lucha contra el *spam* en general aconsejan que nunca se debe actuar perdiendo la ética o la superioridad moral contra los sitios remitentes de *spam* o de contenidos deshonestos, es decir, nunca amenazar con violencia, pagar con la misma moneda efectuando envíos masivos de mensajes, atacar el sitio con métodos de piratería electrónica o *hacking*, ni mediante ningún otro medio no ético. Como ya hemos comentado, los *spammers* a menudo falsifican las cabeceras de los mensajes para ocultar su identidad, y en su lugar añaden la identidad de terceros que son inocentes o que no existen. Por tanto, si respondemos a la dirección origen que aparece en el mensaje con más *spam*, lo único que conseguiremos será causar daños a gente inocente o generar tráfico y colapsar la red.

Tampoco se debe nunca responder al mensaje de correo electrónico no deseado, con el fin de que eliminen la dirección de correo de una supuesta lista. En efecto, en algunas ocasiones el *spam* viene acompañado con una lista de nombres de quien se dice que han expresado su deseo de recibir comunicaciones comerciales, y que puede solicitar la baja de la lista cuando se quiera, pero en realidad a menudo sólo contiene víctimas escogidas al azar, por lo que está incurriendo en un acto ilegal, según las leyes de protección de datos[236]. Otras veces el mensaje *spam* dice que eliminarán su dirección de correo de la lista de usuarios a los que les envía *spam* si así lo solicitan. Pero la realidad es que casi nunca lo hacen, sino todo lo contrario: si se responde solicitando el borrado de la lista, se está confirmando que la dirección está activa. Con esto nuestra dirección de correo será incluida en otra lista de direcciones "activas", es decir, direcciones que existen y que son usadas, con lo que se recibirá más correo electrónico no deseado.

Por otro lado, no debemos dejarnos convencer por los productos, servicios o promociones que se anuncian en el *spam*, ya que en primer lugar se trata de una práctica ilegal, y en segundo, suelen ser actividades fraudulentas o estafas[237].

Lo que se debe hacer es efectuar una queja o denuncia. En ésta se debe incluir la cabecera del *e-mail* (pues como ya hemos comentado[238], contiene los datos que pueden llevar a la identificación del *spammer*), una copia del mensaje original, y los motivos que nos han llevado a efectuar la denuncia. Podemos enviarla al administrador de nuestro proveedor de servicio de correo electrónico o PSI, para que él tome las medidas pertinentes. Su dirección es normalmente postmaster@dominio_PSI o abuse@dominio_PSI.

4.5.1.1. Herramientas disponibles para los usuarios.

Además de efectuar quejas, el usuario debe intentar protegerse del *spam* mediante alguna herramienta de filtrado. Si se utilizan proveedores gratuitos de correo electrónico *web*, éstos casi siempre incluyen alguna. Por ejemplo, Ya.com (Mixmail) ofrece la posibilidad de configurar filtros de correo no deseado dependiendo del grado de seguridad que se requiera para la cuenta (alta, media y baja), y envía los mensajes calificados como "correo no deseado" a una carpeta específica.

[236] Consultar el apartado 3.1. del bloque II, "Breves apuntes sobre legislación y códigos éticos".

[237] Consultar el apartado 2.5., "Ejemplos de estafas y prácticas fraudulentas que realizan los spammers".

[238] Consultar el apartado 3.2., "Análisis del *spam* mediante las cabeceras de los mensajes".

Hotmail también posee una herramienta parecida con la que podemos elegir entre varios niveles de filtrado: "predeterminado", en el que identifica como *spam* los mensajes más claros, "alto" que capturará la mayor parte del *spam*, aunque también puede equivocarse con algún mensaje deseado, y "exclusivo", con el que sólo llegarán a la bandeja de entrada los mensajes de remitentes incluidos en la lista de contactos. Se puede crear una lista negra propia de cada usuario mediante el bloqueo de remitentes. Los mensajes que provienen de estos remitentes o de sus dominios, se eliminan directamente sin llegar a ninguna carpeta de la cuenta del usuario. Así mismo se pueden crear listas de remitentes seguros, cuyos mensajes nunca serán calificados como correo no deseado por el filtro. Un aspecto a tener en cuenta, es que los mensajes que provengan de algunas listas de distribución a las que estemos suscritos, puede que sean calificados como correo no deseado si la configuración de los mensajes en el campo "Para" no es la de nuestra cuenta de correo. Para que esto no ocurra, se presenta la opción de calificar la dirección de la lista como "lista segura". Otra opción interesante para combatir el correo no deseado es la posibilidad de bloquear los gráficos con formato HTML. Es una posibilidad útil para bloquear imágenes ofensivas o dispositivos de rastreo como los *web bugs*, que están basados en imágenes transparentes[239].

Yahoo! por su parte, complementando a las herramientas comentadas para Hotmail, ha desarrollado un dispositivo para reducir la cantidad de *spam* que llega a las cuentas de sus usuarios, denominada Spamguard. Se trata de unas baterías de filtros que se reconfiguran en tiempo real, con ayuda de los propios usuarios. Así, Yahoo! recomienda para ello hacer *click* en el enlace "es *spam*" en todos los mensajes de *spam* que se salten el filtro para estudiarlos e incluir sus remitentes al sistema Spamguard con el fin de ir mejorándolo.

Dejando a un lado el correo *web* o HTML, el cliente de correo más utilizado por el usuario medio (sin conocimientos tecnológicos específicos) es Outlook de Microsoft. Este cliente de correo en su última versión, ha incorporado herramientas específicas contra el *spam*, basadas en filtrar las frases más usadas por los *spammers*. También presenta otra opción que permite marcar un mensaje que no hemos solicitado y automáticamente colocar al remitente en una especie de lista negra propia, para que sea rechazado por el software cuando intente nuevamente enviar un mensaje. Aunque se puede considerar un gran avance, ya que en versiones anteriores la única forma de filtrado que presentaba era la opción de bloquear remitentes, estos tipos de filtrado no son muy efectivos, como hemos venido comentando en este apartado. Sin embargo, existen otras soluciones externas especializadas más efectivas que el usuario puede agregar, e instalar para mejorar las que incorpora Outlook. Tres de las más populares son[240]:

- Spam Attack Pro incorpora una lista de mensajes *spam* a la que se les puede ir añadiendo otros mensajes propios. Puede conseguirse en la dirección www.sofwiz.com/html/*spam*_attack_pro.htm.
- Spam Exterminator (www.unisyn.com/spamex) revisa automáticamente la carpeta de correo en busca de *spam*, de acuerdo con una base de datos de 17 mil direcciones que posee.
- Spamkiller (www.spamkiller.com) es uno de los más completos y puede trabajar con diferentes tipos de filtros: puede detener los mensajes según el remitente, palabras clave, el título o cualquier otra indicación que el usuario especifique.

[239] Consultar el apartado 2.3.2. del bloque II (Web bugs).

[240] "La mayoría de los cibernautas son víctimas del correo indeseado", Tortello M. A., www.aui.es.

Si se desea instalar un filtro bayesiano, también existen varias posibilidades como[241] Spammunition, SpamBayes, Spam Bully, InboxShield, Junk-Out, Outclass, Disruptor OL, o SpamTiger[242].

4.5.2. Acciones desde el punto de vista del administrador de correo electrónico.

El administrador del correo electrónico de una organización que es víctima de *spam*, es el que tiene al alcance de su mano la posibilidad de combatir el *spam* de la forma más efectiva. Por tanto, desde su responsabilidad de administrador, debe estar comprometido con la lucha contra el *spam*, no permaneciendo pasivo ante el problema.

En primer lugar, el administrador debe intentar proteger su organización de los ataques de los *spammers*, acción que puede llevarse a cabo mediante una combinación de las herramientas que hemos venido exponiendo en este apartado. Dependiendo de las características concretas de la organización y de su política, le interesarán un tipo de medidas u otro.

En segundo lugar, el administrador debe atender las quejas de los usuarios, ya sean de su organización, o de usuarios externos. Estas quejas pueden aportar datos de interés a cerca de *spammers*, o incluso informar de que desde su organización se están llevando a cabo actividades relacionadas contra el *spam*. Este último caso sería de extrema gravedad, por lo que deberían tomarse cuanto antes las medidas pertinentes para intentar atajar el problema, definidas por la organización a la que pertenece.

Por otra parte, se debe intentar localizar las direcciones origen del *spam* que ha llegado a la organización. Para ello, hay que tener en cuenta que las cabeceras de los mensajes pueden ser manipuladas y por tanto ser falsas o erróneas. Por ello hay que estudiarlas con atención, con el fin de identificar la verdadera fuente del *spam*, y no dejarse engañar por las posibles direcciones trampa que los *spammers* introducen para ocultar su identidad. En el apartado 2.5., "Análisis de las cabeceras de los mensajes.", se explicó cómo debe llevarse a cabo este análisis.

Si se obtiene la identidad del emisor de *spam*, se debe efectuar una queja o denuncia al responsable del dominio origen, y de la dirección IP origen del *spam*. Las direcciones de correo de dichos responsables, si el dominio o dirección IP están adecuadamente configurados, pueden obtenerse a través de la consulta a la base de datos *whois* que corresponda, como se comentó en el apartado de análisis de las cabeceras (se recomienda su consulta). También pueden enviarse al *postmaster* del dominio origen, cuya dirección puede ser postmaster@dominio_origen o abuse@dominio_origen. De cualquier manera, antes de enviar un mensaje a estas direcciones siempre habría que asegurarse de que existen, comprobándolo mediante una consulta DNS.

Además de a las direcciones que anteriormente se han mencionado, si se trata de *spam* que ofrece servicios de empresas, organismos o individuos españoles a los cuales no se les ha autorizado para que nos envíen comunicaciones comerciales, se debe comunicar este hecho a los organismos pertinentes. Estos organismos son entre otros, la

[241] Graham, P. (2003), "FAQ: Is there a Bayesian Bayesian filter for Outlook?".

[242] Se puede encontrar información adicional de estos filtros en sus páginas web: de "Spammunition" en www.upserve.com, de "SpamBayes" en http://starship.python.net/crew/mhammond/spambayes, de "Spam Bully" en www.spambully.com, de "InboxShield" en www.inboxshield.com, de "Junk-Out" en www.junk-out.com, de "Outclass" en www.vargonsoft.com/Outclass, de "Disruptor OL" en www.disruptor.de, y por último de "SpamTiger" en http://spamtiger.bemat.nl.

Agencia de Protección de Datos (www.protecciondedatos.org) y el Ministerio de Ciencia y Tecnología (www.setsi.mcyt.es), así como a organismos nacionales de lucha contra el *spam*, como la Asociación de Usuarios de Internet (www.aui.es/contraelspam).

Si el *spam* viene de fuera de España, siempre podemos comunicarlo a organismos internacionales de lucha contra el *spam*, como Euro Cauce (www.euro.cauce.org/es/index.html), o Spam Abuse (http://*spam*.abuse.net). Para *spam* procedente de Estados Unidos podemos remitir la queja a la Comisión Federal del Comercio de Estados Unidos (FTC, Federal Trade Commission), en uce@ftc.gov. La FTC por ejemplo, utiliza los mensajes recibidos para perseguir acciones contra la ley de *spammers*.

En la queja o denuncia se debe incluir la cabecera del *e-mail* (pues como ya hemos comentado, contiene los datos que pueden llevar a la identificación del *spammer*), una copia del mensaje original, y los motivos que nos han llevado a efectuar la denuncia. A veces la dirección del emisor del mensaje puede ser la de una persona inocente, que de alguna forma desconoce el proceso que se está llevando a cabo, por lo que el mensaje debería educado y de carácter informativo. También es interesante destacar, que bastantes personas de las que llevan a cabo prácticas abusivas con el correo electrónico, no lo hacen de forma intencionada para molestar, y por ello es importante informarlas y educarlas. Por todo ello es importante realizar las quejas o denuncias en un tono educado y diplomático.

Estas quejas pueden servir como realimentación y ayudar a los organismos de lucha contra el *spam* a tomar medidas contra los *spammers*, a identificar en mejor medida nuevas técnicas de *spam*, etc. En resumen, las quejas y denuncias contribuyen a tomar mejores medidas para combatirlo, ya sea mejorando las herramientas existentes, o desde el punto de vista legal.

Algo que bajo ningún concepto se debe hacer es el bombardeo con mensajes a la dirección de correo electrónico del *spammer*, aunque se tenga la seguridad de que sea ésta verdaderamente. Esta acción tiene varios posibles "efectos secundarios", que son peores que los propios derivados del *spam*:

- Si por casualidad esa dirección no fuera correcta, se estaría bombardeando a un inocente.
- Se pueden producir efectos en otros usuarios de ese proveedor, que nada tienen que ver con el problema.
- Los *spammers* profesionales tiene unos filtros por lo general de mayor calidad, por lo que no les afectará este tipo de bombardeo.
- Se está suministrando direcciones de correo electrónico a una persona que las va a utilizar para enviar basura en el futuro.

Tampoco se debe actuar perdiendo la ética o la superioridad moral contra los sitios remitentes de *spam* o de contenidos deshonestos, es decir, nunca amenazar con violencia, atacar el sitio con métodos de piratería electrónica o *hacking*, ni mediante ningún otro medio no ético, al igual que hemos recomendado a los usuarios.

5. Conclusiones.

El correo electrónico es una herramienta de comunicaciones de gran alcance, usada por millones de personas de miles de formas positivas. Desafortunadamente, al igual que en cualquier situación donde se pueda ganar dinero, también tiene un gran potencial para ser utilizada de manera abusiva.

La proliferación del spam se debe principalmente a que mediante mensajes electrónicos se puede llegar a millones de clientes potenciales sin prácticamente ningún coste. Por ello, aunque las tasas de respuesta del spam sean extremadamente bajas (en torno a 0,0015% o 15 de cada millón), el spam es muy rentable para determinadas personas y negocios. A esto se une la sencillez. En este trabajo hemos comentado cómo sólo es necesario el software adecuado, una conexión a Internet, y una base de datos con las direcciones de correo electrónico de destino. Sin embargo para el resto de la comunidad Internet el spam produce graves daños, por lo que se constituye como uno de los principales usos indebidos que se producen en este medio.

Como hemos venido ilustrando a lo largo de este bloque, el spam representa un abuso para los proveedores implicados en proporcionar el servicio de correo electrónico, que se deriva del afronte de grandes costes económicos. Estos gastos adicionales a los que deben hacer frente, vienen dados por la capacidad de proceso, el espacio en disco y el ancho de banda requerido para la entrega de miles de mensajes; y principalmente, por el tiempo adicional de personal dedicado a solucionar estos problemas, sobre todo en situaciones de saturación. Así, deben hacer frente a la mayor parte del coste de una publicidad que sólo revierte inconvenientes tanto para ellos como para los usuarios.

Por otra parte, también representa un abuso para los receptores de los mensajes, que se ven afectados desde el punto de vista de costes económicos, al tener que hacer frente al gasto (en tiempo y dinero) de la recepción de estos mensajes lo quieran o no, así como de repercusiones sociales. Estas consecuencias en el ámbito social se derivan de la molestia y ofensa asociada a determinados contenidos, y a la inhibición del derecho a publicar la propia dirección en medios como listas de noticias o páginas *web*, por ejemplo, por miedo a que sea capturada. Además, el spam es un freno de la confianza de los internautas, y por tanto para comercio electrónico, Internet, y el adecuado desarrollo de la sociedad de la información en general.

La necesidad de luchar contra este problema ha quedado patente tras la exposición realizada. Sin embargo, la mentalidad tanto de usuarios como de gobiernos no siempre es la adecuada, normalmente por desconocimiento, por lo que es necesaria una gran labor de información y formación en este ámbito.

Así, para intentar frenar el spam es necesario que cada uno pongamos algo de nuestra parte. En primer lugar se debe procurar prevenir el spam dificultando que las direcciones de correo electrónico estén accesibles en las páginas *web*, foros o *chats*, tanto desde el punto de vista de la precaución del usuario cuando utilice alguno de estos elementos, como desde el punto de vista del administrador. Estos agentes juegan un papel importante en la prevención del spam al poder proteger las direcciones de correo electrónico antes de hacerlas públicas, con el fin de que no lleguen a manos de los spammers. En segundo lugar, los proveedores de servicio y administradores de correo

electrónico deben impedir el envío de spam controlando sus sistemas y sus políticas institucionales, para evitar que los recursos que gestionan sean mal utilizados por sus propios clientes o por spammers ajenos al servicio.

Para reducir el impacto que provoca el spam es necesario conocer tanto los efectos y daños que produce, como las herramientas disponibles para combatirlo. En la evaluación de las posibles soluciones habrá que incluir siempre varias alternativas, ya sea desde el punto de vista del usuario o desde el punto de vista del administrador.

Si se es responsable del servicio de correo, se deberán tener en cuenta las características de la empresa y su política, la posible ralentización del sistema de correo, o las necesidades de los clientes a los que se da servicio, etc. La mejor solución pasa por combinar adecuadamente las medidas estudiadas. De esta manera, se debe configurar debidamente el servidor para evitar al máximo el spam que llega, realizando las comprobaciones pertinentes de las transacciones SMTP como primera etapa de filtrado de mensajes, y luego destruir el spam remanente en una segunda etapa con un filtro post-proceso basado en contenidos, preferentemente estadístico o mixto. En el caso de uso de filtros estáticos debemos ocuparnos de la gestión de la base de datos de patrones, que deberá ser alimentada y actualizada continuamente con patrones propios para una mayor efectividad. En el mercado existe un amplio abanico de productos para llevar a cabo estas funciones.

Las medidas basadas en listas negras son también perfectamente viables, aunque desde mi punto de vista son soluciones agresivas porque pueden llegar a rechazar correo legítimo procedente de servidores etiquetados como indeseables. En este sentido es necesario destacar que no nos debemos concentrar sólo en la definición unilateral de listas negras en los servidores, pues si no se coordinan entre sí, el correo electrónico podría deteriorarse más por ello que por los propios problemas que ocasionan los abusos. De esta forma podría llegarse a la nada deseable situación en la que las organizaciones sólo aceptaran mensajes de determinados dominios en base a acuerdos de mutua confianza, y denegar el resto.

Si somos únicamente receptores de spam, debemos utilizar alguna buena herramienta de filtrado e informar periódicamente a nuestro administrador (*postmaster*) del tipo de correo electrónico no deseado que recibimos. Sin embargo, la mejor forma que tiene el usuario de reducir los efectos del spam en sus cuentas de correo es la prevención, de la manera que antes hemos explicado.

En el ámbito de las medidas para combatir el spam desde el punto de vista legislativo, la Unión Europea busca la prohibición de las actividades relacionadas con el problema a través de la aplicación efectiva de la legislación en los Estados miembros, la adopción por parte de las empresas de normas de autorregulación, la sensibilización de los consumidores, y la cooperación internacional. No obstante hemos visto que en algunos países como Estados Unidos, que se encuentran entre los "primeros productores" de correo electrónico no deseado, las leyes no ayudan mucho a prevenirlo ni a erradicarlo. No obstante, el hecho de que exista una legislación que contemple como ilegales aunque sólo sea algunas actividades relacionadas con el spam, constituye un gran paso adelante. Tras haber analizado la situación en este sentido, aunque a priori pareciera que era de vital importancia conseguir que el spam fuera ilegal, ha quedado demostrado que no es ni mucho menos una medida realmente efectiva en la práctica (por lo menos a corto plazo), dada la naturaleza global de Internet, y la imaginación de los spammers ("quien hace la ley, hace la trampa").

Análisis de propuestas acerca de la lucha contra el spam en el futuro.

Hemos estudiado muchas formas de prevenir y combatir el spam, todas en mayor o menor medida igualmente efectivas, pero inefectivas a la vez. Muchos opinan que la única forma de erradicar el spam es conseguir que promocionarse de esta manera no sea rentable.

En este bloque presentábamos que algunas ideas de grandes proveedores para combatir el spam están relacionadas con este punto de vista, y que se baraja la posibilidad de cobrar de alguna manera por los mensajes comerciales enviados. Medidas basadas en esta filosofía podrían conseguir compensar los gastos de los proveedores, y conseguir evitar algún tipo de spam que intenta promocionar negocios fraudulentos. Pero lo que no conseguiría es evitar los daños y molestias que se causa a los usuarios, pues se legitimaría que determinadas compañías realizaran sus promociones a través de envíos masivos.

En una línea similar los gobiernos, con la aprobación de leyes contra el spam, intentan frenarlo a través de multas e incluso condenas a prisión, que hagan del spam una actividad no rentable.

Pero si existe alguna forma de conseguir que el spam no sea rentable es desde el punto de vista del usuario. Las tasas de respuesta están alrededor de 15 por millón. Y este es el problema real, pues los spammers desperdician el tiempo y dinero de un millón de personas para buscar a los 15 más crédulos o más pervertidos que están entre ellos y responden a las ofertas de los productos o servicios que se les ofrecen. Una forma de conseguir que los usuarios no respondan al spam es la educación y la concienciación, pues hemos visto que a menudo los usuarios no están lo suficientemente informados a cerca de las repercusiones del problema. La segunda clave podría encontrarse en la idea de conseguir que los mensajes no lleguen a los receptores, y así éstos no los respondan. Esto puede lograrse mediante filtros. Sin embargo, el tipo de usuario al que va destinado el spam tal vez no use filtros y mucho menos sofisticados. Es más probable que tenga su dirección de correo electrónico con un gran proveedor gratuito como Hotmail, Yahoo!, etc. Por tanto las medidas contra el spam que tomen estos grandes proveedores son de suma importancia.

Si por una parte los usuarios se concienciaran del problema y de sus consecuencias, y por otro, los diferentes métodos de filtrado eliminasen gran parte del spam, tal vez se conseguiría que esta actividad no fuera rentable para determinados spammers. Veámoslo con un ejemplo numérico. En este trabajo dimos cifras de los honorarios de un spammer, que estarían en torno a los 22.000 euros por enviar mensajes a una lista de 250 millones de direcciones. Si los filtros y la concienciación de los usuarios redujeran la tasa de respuestas en un factor de 100 (equivalente a una tasa de acierto de los filtros del 99%), el valor medio de lo que el spammer cobraría por su envío masivo se reduciría a 220 euros, que probablemente ni siquiera cubra los costes de los envíos, pues éstos son bajos pero no en muchos casos no en esa medida. Por tanto un mensaje a todos los usuarios de correo electrónico: *«nunca compres o visites algo que haya sido anunciado mediante spam, si no, estarás siendo cómplice del problema»*.

No obstante, conseguir que los spammers no obtengan beneficios por cualquiera de las vías analizadas es muy complicado, sobre todo si se trata de envíos más pequeños a los que acabamos de hacer alusión, que pueden efectuarse con las conexiones a Internet usuales y por tanto con un coste no superior a 30 euros.

En mi opinión…

No existe una solución clara al problema, por lo que todos los afectados (incluyendo los proveedores de servicio de Internet, la industria del software, las compañías anunciantes, los gobiernos, los internautas y las asociaciones de usuarios) deberían aunar sus esfuerzos en la misma dirección para luchar contra el spam. Trabajando juntos se facilitaría el intercambio de ideas, la discusión del problema y la difusión de la información adecuadamente, que ayudaría a definir una estrategia común a seguir y a aplicar un paquete de soluciones. En la actualidad, cada uno de los agentes nombrados intenta poner soluciones por su cuenta, y por ello no son eficaces.

La clave está en la aplicación de manera coordinada de todas las medidas de prevención y de lucha explicadas, mejorando de forma conjunta algunas como la legislación, y el software de filtrado. También introduciendo otras, como la creación de un organismo central de control de anunciantes y usuarios (un organismo de autorregulación), en el que se velara por el cumplimiento de unas determinadas normas. Asimismo sería positivo que se iniciara una campaña de educación para usuarios, y sobre todo para las compañías, de los daños reales que ocasiona el spam y de las alternativas existentes.

6. Bibliografía.

6.1. Estudios.

- "4ª encuesta a Usuarios de Internet de la AIMC febrero 2001" y "5ª encuesta a Usuarios de Internet de la AIMC febrero 2002", www.aui.es.
- "Consumer Attitudes Regarding Unsolicited Commercial Email (Spam)", octubre-diciembre de 2003. Realizado por TACD (Transatlantic Consumer Dialogue), www.tacd.org/docs/?id=225.
- Encuesta sobre el *spam* realizada por la Asociación de Usuarios de Internet (AUI) a través de su página *web* (www.aui.es) entre abril y mayo de 2003.
- Estadísticas obtenidas del sitio *web* www.xtdnet.nl/paul/*spam*/, Paul Wouters.
- "False Claims in Spam, a report by the FTC's Division of Marketing Practices", abril de 2003, Federal Trade Commission (www.ftc.gov).
- "IV Estudio sobre el Marketing y la Publicidad Medios Interactivos 2002. AGEMDI-fecemd" (Asociación de Agencias de Marketing Directo e Interactivo-Federación Española de Comercio Electrónico y Marketing Directo); www.fecemd.es.
- "Spam E-mail and Its Impact on IT Spending and Productivity" (diciembre de 2003), Spira, J. B., realizado por Basex Inc., www.basex.com.
- "Why Am I Getting All This Spam? Unsolicited Commercial E-mail Research", marzo de 2003, Center for Democracy & Technology de la UE (www.cdt.org/speech/*spam*/030319spamreport.shtml).

6.2. Artículos.

- "Bruselas contra el '*spam*'", Reuters, www.elmundo.es/navegante.
- "Diez recomendaciones de Symantec para luchar contra el *spam*" (6 de junio de 2003), www.noticiasdot.com.
- "Dos de cada tres correos basura son un fraude, según un informe de la Comisión Federal de Comercio de EEUU" (30 de mayo de 2003), www.efe.com.
- "Dos tercios del '*spam*' que recibimos es fraudulento" (30 de abril de 2003), www.iblnews.com.
- "EEUU limita el *spam*" (24 de noviembre de 2003), www.vunet.com.
- "El 55,1% de los mensajes de correo electrónico de EEUU son '*spam*'" (3 de junio de 2003), www.iblnews.com.
- "El Congreso de USA aprueba ley 'anti-*spam*'" (24 de noviembre del 2003), www.conocimientosweb.net/dt.
- "El correo basura colapsará los '*e-mails*' durante un tiempo" (3 diciembre 2002), www.iblnews.com.

- "El *spam* a los clientes será legal en España", www.noticiasdot.com.
- "El '*spam*' cuesta 20.000 millones de dólares a las empresas en todo el mundo", (30 de diciembre de 2003), www.elmundo.es/navegante.
- "El '*spam*' supera por primera vez la mitad del total de correos electrónicos", AFP, www.elmundo.es/navegante.
- "El volumen del correo masivo amenaza el futuro del '*e-mail*'" (1 de mayo de 2003), Iblnews, Agencias. www.iblnews.com.
- "Email Address Harvesting: How Spammers Reap What You Sow" (noviembre de 2002), www.ftc.org.
- "En Gran Bretaña el envío de SPAM es un delito" (19 de septiembre del 2003), www.conocimientosweb.net/dt.
- "Estados Unidos aprueba ley de regulación del Spam" (2 de diciembre de 2003), Guillem Alsina, www.diariored.com.
- "Europa prohibirá el *spam* a partir de otoño", Sánchez, Y., www.diarioenred.com.
- "Evaluación de Alternativas para Reducir el Spam", Sanz de las Heras, J. (mayo de 2000), www.rediris.es.
- "FAQ: Is there a Bayesian filter for Outlook?", Graham, P. (2003).
- "Filters vs. black list" (septiembre de 2002), Graham, P., www.paulgraham.com.
- "For Bulk E-Mailer, Pestering Millions Offers Path to Profit" (13 de noviembre de 2002), Mangalindan, M. del Wall Street Journal, www.alanluber.com.
- "Frequently asked questions about *spam*", Hazen Mueller, S., Panitz A. R., www.spamabuse.net.
- "¡Guerra al Spam!" (5 de febrero de 2004), Guillem Alsina, www.diariored.com.
- "Inside the *spammer*'s world", Livingston, B. (29 de junio de 2001); http://news.com.com.
- "Internautas, empresas y legisladores se unen contra la plaga del correo basura" (22 de mayo de 2003), www.iblnews.com.
- "La Comisión Europea declara la guerra al *spam*" (23 de enero de 2004), www.vunet.com.
- "La Fecemd advierte sobre la legislación de *e-mails* publicitarios" (09 de diciembre de 2003), www.fecemd.org.
- "La Lucha contra el Envío Masivo de Correos no solicitados (spams)", Burgess, T., www.aui.es.
- "La mayoría de los cibernautas son víctimas del correo indeseado", Tortello M. A., www.aui.es.
- "La UE anuncia medidas contra el '*spam*' por la desconfianza que causa" (27 de enero de 2004), Europa Press, www.elmundo.es/navegante.
- "Las cifras del correo basura", A. B. F., www.elmundo.es/navegante.
- "Legisladores británicos planean extraditar a quienes envíen *spam*" (30 de octubre del 2003), www.conocimientosweb.net/dt.
- "Legisladores de Estados Unidos legaliza el *spam*" (27 de noviembre del 2003), http://www.conocimientosweb.net/dt.
- "Los internautas esconden sus direcciones email por miedo al "*spam*"", www.noticiasdot.com.
- "Los productos de consumo y de salud son los que más utilizan el Spam", www.noticiasdot.com.
- "Luchando contra la publicidad no deseada (o Spam) en el correo" (1 de febrero de 2003), Katja y Guido Socher, LinuxFocus.org, http://www.linuxfocus.org/Castellano /January2003/article279.shtml.

- "Make'em pay" (12 de febrero de 2004), www.economist.com.
- "¡Muerte al *spam*!" (30 de abril de 2003), Rodríguez, G., www.libertaddigital.com.
- "Multan a un '*spammer*' con 93.000 euros tras aceptar los cargos" (14 de mayo de 2003), www.iblnews.com.
- "Riesgos del *spam*", Van der Reis,J., www.vanderreis.com/Glosario/riesgosSPAM.htm.
- "Rompe las Cadenas", Campaña contra el Correo Basura, www.aui.es/contraelspam.
- "Sobre la Realidad de Hacer E-commerce V (o El Spam, ¿Violencia contra el Usuario?)" (diciembre 2003), Iriarte Ahon, E., www.diariored.com.
- "¡Socorro! ¡Me ahogo en E-Mails basura!" (30 de junio de 2003), Fleming, P., www.fecemd.es.
- "Spam king lives large off others' *e-mail* troubles" (22 de noviembre de 2002), Wendland, M., www.freep.com/money/tech/mwend22_20021122.htm.
- "¿Spam sí o *spam* no? Legalidad" (26 de agosto de 2003), Hernández, J., www.baquia.com.
- "Técnicos y gobiernos sacan la artillería pesada contra el "*spam*"", Molist, M. ((c) 2003), www.aui.es.
- "The Email Abuse FAQ", http://members.aol.com/emailfaq/emailfaq.html.
- "The Great Spam Supply Chain" (15 de marzo de 2003), Scalet, S. D., www.cio.com/archive/031503/tl_email.html.
- "Winning the War on *spam*: Comparison of Bayesian *spam* filters", Graham, P. (agosto de 2003), www.paulgraham.com.
- Documentación de la conferencia "Internet Level Spam Detection and SpamAssassin 2.50", Sergeant, M. (Senior Anti-Spam Technologist, 2003), MessageLabs, obtenido de www.spamconference.com.
- Documentación de la conferencia "The *spammer*'s compendium", Graham-Cumming (2003), http://popfile.souceforge.net, obtenido de www.spamconference.com.
- Documentación de la conferencia "Spam Filtering. *From* the Lab to the Real World", Goodman, J., Microsoft Research. Obtenido de www.spamconference.com.
- Tutorial sobre Postfix, 2004-02-02, http://hal9000.eui.upm.es/halwiki/Postfix).
- Tutorial sobre Sendmail, www.seguridad.unam.mx/Tutoriales/Tutoriales/sendmail/sendmail.html.

6.4. Otras páginas web de interés.

- http://www.abuse.net.
- http://www.aui.es.
- http://www.aui.es/contraelspam.
- http://www.cauce.org y www.euro.cauce.org.
- http://www.dnsstuff.com.
- http://www.europa.eu.int/comm.
- http://www.europa.eu.int/pol/infso/index_es.htm.
- http://www.exim.org.
- http://www.ftc.gov.
- http://www.ftc.gov/bcp/conline/edcams/*spam*/index.html.
- http://www.ftc.gov/openrelay.

- http://www.internautas.org.
- http://www.mail-abuse.org.
- http://www.messagewall.org.
- http://www.ordb.org.
- http://www.postfix.org.
- http://www.procmail.org.
- http://www.razor.sf.net.
- http://www.rediris.es.
- http://www.rediris.es.
- http://www.rompecadenas.com.
- http://www.samspade.org.
- http://www.sendmail.org/antispam.html.
- http://www.spamassassin.org.
- http://www.spambouncer.org.
- http://www.spamcop.net.
- http://www.spamhaus.org.
- http://www.spamlaws.com.
- http://www.tuxedo.org/~esr/bogofilter.
- http://www.unicom.com/sw/blq.
- http://www.vanderreis.com.