Resumen.

Este trabajo ha intentado clarificar qué es el comercio electrónico desde sus implicaciones más básicas, con el fin de sentar los fundamentos para estudiar las prácticas actuales del marketing en Internet. El objetivo principal ha sido poder hablar en términos propios del marketing, analizando desde el punto de vista ético y legal sus herramientas de comunicación a través de Internet con cierto rigor y comprender qué es lo que se persigue con algunas prácticas de los agentes de marketing. Como caso de estudio especial, se analiza el problema del *spam* o correo electrónico basura.

Para desarrollar estos temas, el proyecto se ha dividido en tres bloques principales: "análisis preliminar del comercio electrónico", "análisis de las técnicas de comunicación mediante Internet" y por último, "el abuso por excelencia de la publicidad *on line*: el *spam*".

1. Análisis preliminar del comercio electrónico.

Una red mundial de comunicaciones mediadas por un gran poder computacional tiene implicaciones en la economía que aún no alcanzamos a evaluar completamente. Por ello las compañías tratan de posicionarse en este nuevo medio probando hipótesis por medio de "modelos de negocio electrónicos", en los que a menudo no son aplicables las estrategias tradicionales. Internet y sus tecnologías asociadas dan al comercio interesantes posibilidades, tanto desde el punto de vista de proveedores como de consumidores. El comercio electrónico puede clasificarse en distintos esquemas desde dos puntos de vista, que explicamos a continuación.

Clasificación según los agentes que intervienen en la transacción.

Dependiendo de los agentes que intervienen en la relación de intercambio, podemos distinguir varias formas de relaciones. Las dos más interesantes para este trabajo son:

- B2B (*business to business*) o comercio electrónico entre empresas. Es el que más desarrollado se encuentra, representando en volumen de negocio alrededor del 75% del total de las transacciones *on line* en España. Para las compañías significa unas oportunidades importantes de crecimiento y sobre todo de posicionamiento. Como dato significativo, hay que destacar que Estados Unidos se halla muy por delante de

Europa en el progreso de estas actividades, y que España se sitúa tras la media europea.

- B2C (*business to consumer*) o relaciones entre empresa y consumidor final. Las actividades relacionadas con esta forma de comercio electrónico están menos desarrolladas. El análisis de su situación nos la presenta como un fenómeno extendido y con un gran potencial futuro, pero todavía en fase emergente. Una de las causas de ello es la baja penetración de Internet en la sociedad española. No obstante, se está experimentando un alto crecimiento en número de usuarios (en torno al 10% anual, que constituía ocho millones de internautas a principios de 2003), y aunque en menor medida, un cambio en su mentalidad que hace que se vayan adaptando a las nuevas tecnologías.

En el ámbito del B2B, las cifras y los estudios nos han indicado la rentabilidad del posicionamiento *on line*. Sin embargo, la situación de las empresas dedicadas al B2C cuyos ingresos provienen únicamente de su presencia en Internet es difícil, puesto que muchas compañías se aventuran a negocios electrónicos por percibirlo como un medio que aporta numerosas ventajas, sin darse cuenta que en la realidad exige gran competitividad. La diferencia viene dada por el gran número de compañías que compiten globalmente intentando obtener beneficios, y la baja penetración y uso del comercio electrónico por los usuarios, al contrario que en los negocios entre empresas.

Los principales frenos del desarrollo del comercio electrónico al consumidor final son los problemas detectados por los usuarios en su contacto con la red, por un lado tecnológicos (la calidad de las comunicaciones y el coste telefónico), y por otro, la falta de confianza en el medio Internet, que viene dada por la percepción de inseguridad en las transacciones (miedo a dar los datos personales, desconfianza en el medio de pago,...) y por la publicidad no deseada.

Clasificación según el modelo de negocio.

Por otra parte, las actividades de comercio electrónico pueden clasificarse dependiendo de en qué modelo de negocio estén basadas, es decir, de qué forma la empresa genera ingresos a través de su posicionamiento en la cadena de valor. Así, los modelos de negocio son el modo concreto en el que se plasman los distintos tipos de comercio electrónico desde el punto de vista de la obtención de beneficios. Desde este enfoque podemos diferenciar los siguientes modelos:

- "empresa productora",
- basados en la venta,
- de e-aprovisionamiento,
- de intermediación,
- de proveedor de servicios de Internet,
- fundamentados en la publicidad,
- y de suscripción.

Es importante destacar que dos de los tres modelos de posicionamiento orientados al consumidor final mencionados (de publicidad y de suscripción), se basan en los ingresos por publicidad, y en la explotación de la información de los usuarios con fines de marketing. Esto es de vital importancia para el tema central de este proyecto, y nos sirve de punto de partida para el análisis que hemos llevado a cabo, y cuyo resumen vamos a exponer, junto con las formas de promoción y la obtención de datos de los usuarios mediante Internet.

2. Análisis de las técnicas de comunicación mediante Internet.

Una nueva forma de comercio, un mercado más exigente, global y preparado, y una competencia cada vez más afilada, se presentan ante el marketing como consecuencia directa de la revolución tecnológica que ha propiciado Internet. Este mercado global, que sirve como soporte a la economía digital, está desarrollando sus propios modelos de negocio, como hemos comentado, y también sus técnicas de marketing. En este trabajo nos hemos centrado en la comunicación, y en concreto en las formas de publicidad y en la obtención de datos de los internautas, cuyos objetivos son en último término incrementar las ventas de la empresa.

Del análisis sobre comercio electrónico efectuado en este trabajo, obtuvimos que hoy día alrededor de ocho millones de españoles tienen acceso a Internet, lo que lo convierte en un medio de comunicación con una audiencia potencial muy relevante. Más importante aún es su ritmo de crecimiento, que sigue siendo superior al 10% anual. El perfil "tipo" del internauta tiene un medio-alto poder adquisitivo y sociocultural, por lo tanto los anunciantes pueden alcanzar a un público objetivo muy interesante con un precio infinitamente menor que mediante otros medios de promoción tradicionales.

Otra de las principales ventajas que aporta Internet al mundo del marketing, es que ofrece una mayor precisión a la hora de obtener datos estadísticos de los usuarios, es decir, información acerca del perfil poblacional de su audiencia (donde vive, cuáles son sus preferencias, incluso hasta su dirección de correo electrónico), y ofreciendo la posibilidad de analizar casi en tiempo real los resultados de la campaña. Esto permite al empresario poder conocer cuántas personas visitan diariamente su *web* y qué porcentaje realiza una compra después de conocer los productos en la red. De esta manera Internet permite al marketing personalizar la comunicación, es decir, que cada individuo reciba un mensaje diferente según sus preferencias. Además, da la oportunidad de enviar un determinado anuncio justo a aquellas personas que han demostrado interés por un contenido en concreto.

Hay que destacar que la publicidad en Internet es imprescindible. Por una parte porque toda actividad comercial (ya sea *on line* u *off line*) debe ser conocida por los clientes potenciales para que tenga éxito, no basta esperar a que nos visiten tras haberla puesto en funcionamiento: debemos promocionarla. Por otra parte, la filosofía sobre la que se ha desarrollado Internet es la de "compartir información de forma desinteresada", y en esta línea, una gran mayoría de sitios *web* ofrecen servicios de manera gratuita. La tecnología y los recursos necesarios para ello requieren de fuentes de financiación, que se ven cubiertas en gran medida por los ingresos obtenidos por publicidad (modelo de negocio publicitario).

2.1. Los medios y formatos usados por la publicidad en Internet.

La publicidad *on line* ofrece gran flexibilidad en la creación de campañas publicitarias mediante diversos tipos de anuncios, que hemos clasificado basándonos en cómo se presentan: si el internauta de algún modo acepta o permite la publicidad, o si ésta irrumpe en su navegación sin aviso previo ni consentimiento. De este modo tenemos "formas de publicidad basadas en *push*" y "basadas en *pull*", con sus distintas variantes, que definimos a continuación.

"Formas push".

Se trata de formatos publicitarios en los que el receptor no escoge recibir este tipo de información, sino que le es impuesto en su navegación. Se basa pues en mensajes insertados sin que exista una previa aceptación de la publicidad por parte del receptor. De acuerdo con esta definición, incluimos en dicho grupo los anuncios en forma de rótulos publicitarios y ventanas emergentes (insertados en la web), junto con las técnicas de *e-mail* marketing (sobre correo electrónico).

- Las formas de **publicidad en la *web*** presentan con gran cantidad de variantes: *banners, botones, interstitials, pop-ups, skycrapers, layers, cyberspots* y *shoshkeless,* que mediante un *click* sobre ellos conducen al internauta a otra página con más información del anunciante. Pueden contener gráficos, animaciones, audio, o una combinación de dichos tipos de archivos. En Internet, creatividad y tecnología van de la mano en el desarrollo de los formatos publicitarios. Las posibilidades tecnológicas que nos ofrece el medio permiten la innovación constante y la búsqueda de formatos más notorios que sorprendan al usuario. Este es el caso de los formatos que incorporan tecnologías *rich media*, mediante las cuales el anunciante puede insertar en la página *web* un anuncio del tipo de los de la televisión. Si bien los *banners* y botones aparecen hoy en día como parte del paisaje de la red, los *interstitials*, *pop-ups* y *layers* destacan por su impacto y su capacidad para generar emociones.
- Las técnicas de ***e-mail* marketing**, que pueden ser encuadradas en las formas de promoción basadas en *push* por la propia naturaleza de la recepción de los mensajes, consisten en enviar comunicaciones comerciales vía correo electrónico a receptores que previamente lo soliciten. El *e-mail* marketing también ofrece varias posibilidades en el formato de sus envíos, como los boletines electrónicos o *newsletters* (*e-mails* enviados regular y periódicamente con el fin de mantenerse en contacto con los clientes o suscriptores, mediante la inclusión de contenidos de interés); el envío en forma de promociones, regalos y descuentos especiales; y la inserción de publicidad en los envíos por *e-mail* (ya sea en forma de *banners*, etc o de simplemente unas líneas al final del mensaje).

Formas de promoción "pull".

En este tipo de formatos publicitarios, el usuario no se ve privado de su navegación ni invadido por pantallas ajenas a la que está consultando, sino que se basan en las propias características de la página que en ese momento visualiza, o que tienen algún interés distinto para el internauta que la mera promoción de un sitio *web*. Algunos ejemplos son:

- los aspectos a tener en cuenta en la creación del sitio *web* que contribuyen a darlo a conocer, en el ámbito del diseño y de la programación de la página;
- la promoción mediante el alta en buscadores y directorios;
- a través de enlaces en páginas de otras compañías;
- proporcionando a los usuarios servicios gratuitos o artículos de interés, que de esta forma pueden contribuir a dar a conocer la compañía.

Otras formas de promoción.

Al margen de las anteriores, se detectan en la red otras formas de publicidad de dudosa ética y legalidad, en las que mentes sin escrúpulos se aprovechan de los agujeros de seguridad que detectan tanto en los sistemas operativos como en los navegadores, para llevar a cabo acciones relacionadas con la publicidad. Todas ellas son destacables

por la tremenda violación de la intimidad y abuso de los usuarios que representan. Nos referimos al uso de herramientas como:

- El **Messenger Service** del sistema operativo Windows, cuya aplicación original es el envío de mensajes de sistema por el administrador a sus usuarios para informar de eventos, como puede ser la baja temporal de un servicio. También puede ser usado por el software de la impresora para comunicar el estado de un documento en impresión, por el programa antivirus para advertir de que ha detectado una posible intrusión, etc. Sin embargo últimamente se está utilizando como novedoso formato publicitario agresivo, que se abre sin necesidad de tener el explorador abierto, haciendo pensar al usuario que se trata de algo importante. Estos mensajes son totalmente anónimos, y es imposible rastrear su procedencia.
- Otro ejemplo es el uso de **códigos maliciosos o virus**, que pueden ser utilizados con el objetivo de predisponer al usuario a recibir publicidad de forma masiva por parte del creador del código. También para la recopilación de direcciones de correo electrónico por parte de *spammers,* o para manipular las máquinas de los usuarios para que emitan publicidad. Estos últimos casos son los de los virus Sobig y Mydoom, que convertían los ordenadores de los usuarios en fuentes de *spam*, y recopilaban todas las direcciones de correo electrónico de las carpetas de contactos de los usuarios.

Análisis desde el punto de vista ético y legal.

Aunque el marketing nunca persiga incomodar a un posible usuario potencial, algunos de los formatos publicitarios de los que hemos hablado pueden hacer que el internauta se sienta invadido y considere la publicidad como intrusiva, pues en muchas ocasiones la gran cantidad de basura recibida, llega incluso a imposibilitar una navegación fluida. Pero al menos las dos primeras formas de promoción comentadas, pueden considerarse de alguna forma "legítimas". Sin embargo en el caso de los últimos métodos expuestos (el uso de códigos maliciosos y el Messenger de Windows), se viola la intimidad de los internautas y se causan terribles daños:

- Económicos, por la necesidad de limpieza de los ordenadores de los usuarios de la gran cantidad de software basura que impide el buen funcionamiento de sus máquinas, así como por la necesidad de uso de software antivirus.
- Sociales, ya que este tipo de prácticas repercuten en que la imagen que los usuarios se hacen de Internet es de un mundo caótico. Esto redunda en una tremenda falta de confianza y por ello frena el uso de Internet para aplicaciones de importancia (como el comercio electrónico), al menos en los usuarios con menos conocimientos tecnológicos.

En esta misma línea, otras formas como el *spam*, derivado del *e-mail* marketing, se constituye como uno de los métodos de promoción más abusivos al utilizar recursos ajenos para inundar los buzones de los internautas con mensajes no deseados. Se trata desde mi opinión de uno de los mayores abusos de Internet, por lo que ha sido analizado en profundidad, dedicándose a ello el siguiente apartado al completo.

El tema de la publicidad intrusiva representa un debate abierto hoy en día, que pone en tela de juicio la ética de la publicidad *on line* y su legalidad. La situación actual de la legislación no penaliza la mayoría de los abusos en este ámbito, aunque sí la publicidad engañosa o los contenidos ilícitos. Por tanto, las posibles soluciones a este problema van por la vía de la autorregulación, cuyos códigos son más versátiles y cercanos a los problemas reales que se presentan a los internautas que la legislación.

2.2. La obtención de datos de los usuarios con fines de marketing mediante Internet.

Como ya hemos comentado, una de las principales ventajas de la publicidad en Internet es el hecho de poder conocer datos de cada usuario específico. Sobre esta premisa se basan las técnicas de marketing relacional, en las que con los datos obtenidos, la compañía se puede dirigir al usuario de una manera más personalizada, discriminando el público objetivo al que le interesa impactar, y obteniendo una comunicación dirigida que rentabiliza al máximo sus impactos. También pueden utilizarse para facilitar la navegación de los internautas, pues posibilita una mejor transacción de las peticiones realizadas por los usuarios.

La exhaustiva medición de la audiencia de un espacio permite evaluar la efectividad de un sitio *web* o de las diferentes acciones de promoción, así como conocer quién es el público objetivo de una página, cuáles son aquéllas de más éxito y detectar qué funciona y qué no. Gracias a la información obtenida, se pueden realizar tests previos que certifiquen la posterior efectividad de la campaña y monitorizar en tiempo real los resultados que está teniendo.

En el ámbito del uso de estos datos para la confección de perfiles detallados de los internautas, es especialmente importante el decidir hasta qué punto se puede llegar sin la violación de la intimidad y la vulneración de sus derechos más elementales. Estos datos del usuario pueden llegar a ser tan concretos como el país, la región y el proveedor desde el que accede; las páginas visitadas, el tiempo de permanencia en cada una y la hora; el sistema operativo y el software instalado en su ordenador, etc.; e incluso la dirección de correo electrónico y las contraseñas guardadas en memoria. En muchos casos como éstos, la línea divisoria entre el desarrollo de las actividades de marketing y el respeto a los usuarios queda difuminada y muchas veces traspasada.

Algunas alternativas disponibles para la obtención de datos.

Existen muchas instituciones y herramientas tecnológicas que están dedicadas a obtener datos de los internautas:

- Hay diferentes **organismos y empresas** que trabajan para descubrir el perfil de las audiencias en Internet, lo que permite que los anunciantes dispongan de información legítima, fiable y contrastada acerca de los diferentes soportes digitales. Entre ellos, se encuentran la OJD (Oficina de la Justificación de la Difusión), el EGM (Estudio General de Medios), Nielsen-NetRatings, Taylor Nelson Sofres, MMXI (perteneciente a Forrester Research),… Estos organismos utilizan para la recopilación de datos técnicas como el panel de navegantes, encuestas, cuestionarios en la web y auditorías de actividad.
- Por otro lado, las compañías de marketing tienen a su disposición todo un abanico de **herramientas software específicas** para este fin. Un ejemplo de ellas son los *trackers*, que son una forma de medición externa al sitio, realizada por un tercero que funciona como certificador.
- Existen formas de obtención de datos derivadas del funcionamiento intrínseco de Internet, y que aunque están siendo empleadas con fines de marketing, el uso propio de ellas no tiene nada que ver. Un ejemplo son las bases de datos *whois,* y los ficheros *Hosts.txt* y *.log* de los servidores. En el caso de los últimos, los datos que se obtienen son de los servidores de la propia compañía (como qué páginas visita el internauta, número de usuarios,…), de naturaleza estadística, y no están relacionados con datos personales.

Otras herramientas. Aspectos éticos y legislación.

Mediante Internet, pueden utilizarse otras herramientas de obtención de datos que representan un abuso, puesto que obtienen datos de los internautas sin que éstos conozcan el proceso que se está llevando a cabo. Un ejemplo de ellas son los *web bugs,* los programas *spyware*, y los *cookies* en algunas ocasiones.

- **Los *cookies*** son una herramienta que posibilita a la empresa que los fija, la monitorización de los hábitos de navegación en de los internautas en esas páginas *web* concretas. El usuario puede aceptarlos o rechazarlos a través de su navegador, por lo que, aunque los datos recabados pueden llegar a ser relevantes, en teoría gozan del consentimiento del usuario, y por tanto, no representarían un gran problema. Sin embargo, el usuario pocas veces sabe de qué se trata, por lo que la aceptación de concesión de estos datos se da realmente sin el conocimiento del usuario.

  Al margen de su uso "legítimo", existen agencias de publicidad *on line* que "trafican" con la información recopilada a través de *cookies* por cientos de sitios *web*, incluso asociándola a datos personales de los usuarios. Este caso, representa un grave abuso y violación de las leyes de protección de datos, desde cualquier punto de vista.
- Un ***web bug*** (insecto del *web* o también llamado baliza) es una imagen transparente de un píxel incrustada en un documento HTML, es decir, una página *web* o un mensaje de correo electrónico en este formato. Cuando el internauta navega o accede a una página que contiene el *web bug,* éste envía su dirección IP de nuevo al servidor del anunciante. Este procedimiento se utiliza a menudo junto con los *cookies*, de forma que examinando el *cookie* y los datos enviados por el *web bug*, el anunciante puede reconocer al internauta a través de cualquier sitio en el que posea un anuncio y enviar información sobre la actividad del usuario en la red. En este aspecto, su finalidad es parecida a la de los *cookies* (pueden ser usados para seguir los movimientos de los internautas a través de la red), pero son más difíciles de localizar y mucho menos de consentir o aceptar, siendo imposible con un navegador convencional o a simple vista.
- Los **archivos espías o *spyware*** son diminutas aplicaciones que se instalan en el ordenador del internauta sin su conocimiento. Su objetivo es la recogida de datos del sistema donde están instalados, para su posterior envío a aquel que controla el *spyware,* mediante la utilización subrepticia de la conexión a la red del usuario afectado. Existen varios tipos, pero el que nos compete es el software publicitario o *adware,* que se utiliza para determinar todo tipo de datos que indiquen la conducta y hábitos del internauta con fines publicitarios. Sus efectos son por una parte la violación de los derechos de confidencialidad de los datos y de la intimidad del internauta. Por otra, una navegación y funcionamiento del ordenador más lentos, producidos porque estos programas están continuamente ejecutándose. Ello hace que al ordenador le quede menos memoria libre para trabajar y que funcione con dificultades, sobre todo al iniciar el equipo. La navegación también se ralentiza, debido a que los procesos se ejecutan más despacio, y a que además, roban los recursos de conexión a la red y el ancho de banda disponible.

Con todo lo anterior, la combinación de las diversas técnicas de archivos espías y otras herramientas establecen una corriente de datos en ocasiones bastante relevantes como para que nadie quisiera facilitarlos indiscriminadamente. La utilización de estos datos por parte de empresas de marketing, supone para las mismas una actividad lucrativa difícil de eludir por el usuario, que se encuentra indefenso principalmente por desconocimiento del proceso, el cual se realiza de forma "subterránea".

La única defensa legal con la que cuenta el usuario es **la LOPD (Ley Orgánica de Protección de Datos)**. Esta ley considera dato personal a toda información que se refiera a personas identificadas o identificables. Así, si alguna de las herramientas mencionadas obtiene algún dato que se asocia con datos personales del usuario (que pueden ser nombre, dirección de correo electrónico, dirección o dirección IP, etc), su contenido puede ser a su vez considerado como dato personal. Por tanto, al recabar la información, deben cumplir lo especificado por la ley: proporcionar información de la compañía que recoge los datos, así como los aspectos necesarios para poder ejercer los derechos de consentimiento, acceso, cancelación, oposición y de especificación de las finalidades para las que autoriza el uso de los datos.

Sin embargo el proceso de cumplimiento de ésta, si se da, suele tener lugar en situaciones en las que el usuario realmente no da ningún tipo de consentimiento: lo que las compañías suelen hacer es incluir cláusulas lo suficientemente amplias en sus políticas de privacidad o contratos, que les cubran desde el punto de vista legal, pero que el usuario a menudo desconoce.

Lo realmente perjudicial de estos sistemas es lo referente a la violación de la intimidad del usuario. La legislación en torno a la protección de datos podría considerarse aceptable al menos en lo que concierne a empresas de la Unión Europea, por lo que el usuario estaría más o menos protegido, o en todo caso con el derecho a denunciar estos abusos. En España, el hecho de que el gobierno promueva la autorregulación y con ello se haya creado un código ético por parte de la entidad Confianza OnLine, me parece un gran paso adelante para intentar regular, controlar y frenar estas prácticas, que van en perjuicio del internauta, y por tanto de un Internet seguro y fiable. No obstante la autorregulación y sus posibilidades son un tema muy poco conocido, tanto por los usuarios como por las compañías, lo que la hace poco efectiva, al menos por el momento. Por otro lado, la situación de otros países como por ejemplo Estados Unidos, donde las leyes de protección de datos son prácticamente inexistentes, las compañías tienen casi vía libre para espiar cuanto deseen a los internautas, algo bastante preocupante.

2.3. Conclusiones de la valoración ética y legal de algunas actividades de marketing *on line*.

La publicidad y la obtención de datos en Internet son imprescindibles y presentan muchas ventajas respecto a estas actividades en otros medios. Sin embargo no siempre esta publicidad es inofensiva, ni está concebida desde el respeto a los usuarios ni a sus intereses. Con esto nos referimos a que las compañías de marketing *on line* llevan a cabo una serie de abusos contra los usuarios que a veces deberían ser intolerables, y que la legislación a menudo no contempla.

Aún más grave son los abusos que se dan en torno a la obtención de datos de los usuarios, que sobrepasan los límites de la legalidad. Los usuarios (y sobre todo las asociaciones de consumidores) deberían denunciar estas prácticas, lo que podría ayudar a que los organismos oficiales intervinieran para prevenirlas o castigarlas tomando las medidas oportunas en cada caso en concreto. Sin embargo, el internauta a menudo no posee los conocimientos tecnológicos ni culturales para llevar a cabo estas acciones, por lo que se encuentra totalmente desprotegido.

3. El abuso por excelencia de la publicidad on line*: el* spam*.*

3.1. Ante qué problema estamos.

Denominamos *spam* o correo electrónico basura a las comunicaciones comerciales no solicitadas realizadas a través de correo electrónico u otros medios electrónicos equivalentes, y al envío masivo de mensajes no solicitados, sean o no comerciales. No hay lugar a dudas de que, junto con los virus, el *spam* es en la actualidad uno de los principales problemas de Internet, pues un porcentaje cada vez más alto de todos los mensajes de correo electrónico que se envían y reciben (a fecha de febrero de 2004 era del 62%) son anuncios de Viagra, de páginas pornográficas o de programas informáticos con el precio muy rebajado, porque son "piratas".

El correo electrónico es una herramienta de comunicaciones de gran alcance, usada por millones de personas de decenas 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 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**.

- Obliga a afrontar grandes costes económicos a los proveedores implicados en proporcionar el servicio de correo electrónico, que vienen dados por:
  - el consumo de capacidad de proceso, espacio en discos de almacenamiento 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 costear la mayor parte de una publicidad que sólo revierte inconvenientes tanto para ellos como para los usuarios.
- También representa un abuso para los receptores de los mensajes, que se ven afectados desde el punto de dos puntos 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;
  - de repercusiones sociales, que 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.

En consecuencia, la tendencia de crecimiento exponencial que está experimentando el *spam* podría llegar incluso a inutilizar el servicio de correo electrónico tal y como es conocido actualmente.

3.2. Métodos de lucha contra el *spam*.

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, lo que pone de manifiesto que es necesaria una gran labor de información y formación en este ámbito. Para combatir de forma eficaz el *spam* es necesario trabajar desde diferentes niveles, en cada eslabón de su cadena de distribución según esté en nuestras manos, es decir, ya seamos usuarios (receptores del *spam*), creadores de contenidos, o proveedores de servicios de Internet.

Prevención.

En primer lugar se debe procurar prevenir el *spam* dificultando que los *spammers* obtengan direcciones de correo electrónico víctimas. Sabiendo que el modo principal en el que las obtienen es rastreando Internet mediante búsquedas selectivas, lo que se debe intentar es que las direcciones no 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 creador o administrador. Estos agentes juegan un papel importante en la prevención del *spam* al poder proteger las direcciones de correo electrónico antes de hacerlas públicas.

En segundo lugar, los proveedores de servicio y administradores de correo electrónico deben **impedir el envío y distribución ilegítima** 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. Existe un gran problema con los servidores mal configurados u *open relays*, puesto que son servidores que permiten a cualquier otra máquina del mundo dirigir mensajes a través de ellos, con destino a otros usuarios de correo de cualquier otra parte de Internet. Estas estafetas son las preferidas por los *spammers* para inyectar sus mensajes, 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. Por tanto, es necesario que el administrador del servicio de correo electrónico conozca el problema e impida la distribución de *spam* a través de sus máquinas.

Combatiendo el spam.

Los gobiernos intentan combatir el spam legislando esta actividad. La Unión Europea prohíbe toda forma de comunicación comercial electrónica no solicitada, salvo la que pueda darse entre una empresa y sus clientes, y busca la erradicación del spam a través de la aplicación efectiva de esta 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. En España se ha llevado a cabo mediante la LSSI. En otros países como Estados Unidos sin embargo, hemos visto tras el análisis llevado a cabo en este trabajo, que las leyes aprobadas no ayudan mucho a prevenirlo ni a erradicarlo. Esta situación representa un gran problema porque se trata de un país que se encuentra entre los "primeros productores" de *spam.*

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. Por otra parte, aunque a priori parezca que es de vital importancia para

erradicar el *spam* conseguir que sea ilegal, la experiencia está demostrando 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").

En una línea totalmente distinta, han surgido algunas **ideas de grandes proveedores** para combatir el *spam* de cara al futuro. Su filosofía está relacionada con conseguir que el *spam* no sea rentable, barajando la posibilidad de cobrar de alguna manera por los mensajes comerciales enviados. Sin embargo, medidas basadas en esta idea podrían conseguir compensar los gastos de los proveedores, y 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.

Herramientas tecnológicas.

Las principales herramientas tecnológicas para combatir el spam se basan en el filtrado del correo entrante para separar el *spam* de los mensajes útiles. Comentamos a continuación las principales.

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**. Si se tienen certezas de que se trata de un mensaje *spam*, la transacción no finaliza con éxito, y por tanto el mensaje es rechazado. Esta decisión se toma en función de la cabecera de los mensajes enviados durante el diálogo SMTP, que describe determinadas características de configuración del servidor origen. También se pueden tener indicios del perfil del servidor que pretende enviar el mensaje comprobando si se encuentra en listas negras, que contienen una serie de máquinas cuya configuración o antecedentes indican que pueden ser emisoras de *spam*.

También existe la posibilidad de filtrar el *spam* que ha traspasado las barreras anteriores en una segunda etapa, mediante **filtros "basados en contenidos"**. Funcionan escaneando los mensajes entrantes en busca de palabras o patrones de texto indicativos de que se trata de un mensaje *spam*. El contenido del cuerpo y cabecera del mensaje entrante es comparado con una base de datos que contiene patrones de mensajes *spam*. Si se dan un número determinado de coincidencias, se califica el *e-mail* como *spam*. Este filtrado se puede realizar tanto desde la máquina del usuario, como a nivel del servidor de correo electrónico. En el mercado existe un amplio abanico de productos para llevar a cabo estas funciones, que pueden clasificarse en dos grandes grupos:

- Los **filtros "estáticos" o "basados en reglas"**, en los que la base de datos que contiene los patrones que determinan la decisión de considerar un mensaje como spam, es fija. Su funcionamiento se basa en que si se detecta al menos un número determinado de aciertos (umbral), el mensaje se califica como *spam*. Para su buen funcionamiento es de vital importancia ocuparse de la gestión y actualización de la base de datos de patrones, que deberá ser alimentada continuamente con mensajes *spam* propios, para una mayor efectividad.
- Los **filtros bayesianos** o adaptativos, en los que la base de datos con los patrones, se genera y actualiza automáticamente a partir de los mensajes recibidos. Están basados en la aplicación al filtrado del Teorema de Bayes de probabilidades combinadas. Su funcionamiento es el siguiente:
    - Estos filtros inicialmente se entrenan con una cantidad de *spam* y de mensajes válidos, para que reconozcan qué mensajes el usuario considera de cada tipo.

- Cuando llega un nuevo mensaje al filtro, este se descompone en palabras y se calculan sus probabilidades de ser *spam*. Esta probabilidad se basa en cálculos que tienen en cuenta cuán a menudo aparece un patrón determinado en *spam* frente a 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 del contenido del cuerpo del mensaje y del contenido de la cabecera.
- En función de estas probabilidades, se calcula la probabilidad global de que el mensaje sea *spam*.
- Si esta probabilidad supera un determinado umbral, el mensaje es calificado como *spam*.
- Finalmente, se actualiza localmente la base de datos con los posibles nuevos patrones y probabilidades asociadas.

De esta forma, cada mensaje que entra es calificado como *spam* o como mensaje legítimo, y a su vez, sigue entrenando al filtro (actualizándose los patrones y las probabilidades), logrando cada vez mejores resultados. Además, esta filosofía hace que el filtro se adapte automáticamente al idioma y al tipo de mensaje recibido. Una vez pasado el periodo inicial de entrenamiento, puede alcanzar una eficacia alrededor del 99,5% con pocos falsos positivos, es decir, mensajes deseados que sean considerados como *spam*.

A modo de **comparativa entre los distintos métodos de filtrado**, podemos decir que el filtrado bayesiano tiene una serie de ventajas respecto al filtrado basado en palabras clave o en listas negras, que se derivan del hecho de que pueden autoadaptarse al correo de cada usuario concreto (con lo que se evita la gestión de la base de datos de patrones) y también a los mensajes indeseados que lleguen, siendo capaz de defenderse dinámicamente ante nuevas técnicas de spam, o diferentes idiomas.

Sin embargo, 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. En contraposición las medidas de filtrado basadas análisis de las transacciones SMTP, evitan la entrada de spam en nuestro dominio, con el ahorro de recursos que esto conlleva. Además, presionan al origen para que no vuelva a intentarlo, ya que éste recibe todos los mensajes de error que se generan al fallar las transacciones SMTP necesarias para entregar cada mensaje. Desde este punto de vista, estas medidas son más comprometidas para luchar contra el problema del spam de raíz. No obstante también son más injustas, puesto que catalogan a un servidor origen sin dar oportunidad a analizar si su mensaje es spam o no.

Consejos.

Para reducir el impacto que provoca el *spam* es necesaria la evaluación de las posibles soluciones, y siempre habrá que incluir varias alternativas:

- Si se es **responsable del servicio de correo** de una institución, se deberán tener en cuenta las características de ésta y su política, la posible ralentización del sistema de correo, las necesidades de los clientes a los que se da servicio, etc. En la mayoría de las ocasiones la mejor solución pasa por combinar adecuadamente las medidas estudiadas.
- Si somos únicamente **receptores** de *spam*, debemos utilizar alguna buena herramienta software 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.

Además, en definitiva los usuarios tienen en sus manos decidir si el *spam* es rentable. Las tasas de respuesta del *spam* son extremadamente bajas, lo que provoca que los *spammers* desperdicien el tiempo y dinero de millones de personas para encontrar un puñado de clientes que responden a las ofertas de los productos o servicios que se les ofrecen. Por tanto es una buena práctica no comprar o visitar algo que haya sido anunciado mediante *spam*.

3.3. Conclusiones acerca de la lucha contra el *spam*.

Hemos expuesto muchas formas de prevenir y combatir el *spam*, todas en mayor o menor medida igualmente efectivas, pero inefectivas a la vez. Es obvio que no existe una solución clara al problema, por lo que la única alternativa para combatir el *spam* de forma eficaz es 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) aunen sus esfuerzos en la misma dirección. 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 a seguir conjunta y a aplicar un paquete de soluciones. En la actualidad, esto no se ha llevado todavía a cabo y cada uno de los agentes intenta poner soluciones por su cuenta, por lo que no se ha conseguido ni siquiera frenar el aumento del *spam*.

La clave podría estar 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. No obstante estamos ante un problema de difícil solución y que representa un gran reto en la expansión y buen funcionamiento de Internet.