UNIVERSITAT POLITÈCNICA DE VALÈNCIA

ESTUDIO DE LOS ASPECTOS LEGALES DEL SPAM

PROYECTO FINAL DE CARRERA

INGENIERÍA INFORMÁTICA

UNIVERSIDAD POLITÉCNICA DE VALENCIA

AUTOR: Oscar Manuel Alapont Cabestrero

DIRECTOR: Juan Vicente Oltra Gutiérrez

Valencia, Septiembre 2011

etsinf

Escuela Técnica
Superior de Ingeniería
Informática

INDICE

1- Objeto y objetivos

El objeto del presente Proyecto de Fin de Carrera es la obtención del título de Ingeniería Informática Expedido por la Universidad Politécnica de Valencia.

Los objetivos del proyecto pretenden hacer un estudio pormenorizado del fenómeno del spam, desde el contexto donde se produce, su origen, cómo es generado y distribuido, los tipos existentes atendiendo a los más importantes y de mayor impacto como *hoax*, *phising*, *suplantación de personalidad* y cualquier tipo de fraude en Internet que es provocado a través de este medio. Se aborda asimismo la problemática derivada del spam, un estudio del impacto que éste causa, y aspectos importantes a tener en cuenta como los agentes implicados en esta problemática, sus posiciones y los sistemas existentes que pueden hacer frente al fenómeno spam.

El presente proyecto incluye el estudio más genérico de spam, dando la visión existente de la publicidad, sobretodo en medios electrónicos, y de las comunicaciones electrónicas comerciales no solicitadas.

Asimismo se realiza un estudio profundo de los aspectos legales del spam, revisando la normativa del ordenamiento jurídico en la materia tanto en España como en Europa, con la elaboración de una guía para el cumplimiento de la legislación española y comunitaria respecto al spam, revisando las obligaciones y derechos de cada una de las partes implicadas en el proceso del envío de comunicaciones comerciales no solicitadas.

Por último se describen los sistemas de autorregulación existentes, así como de la solución extrajudicial de conflictos, y un estudio de las cuestiones deontológicas y éticas relacionadas con la materia.

2- Introducción: Contexto y visión global del spam

Actualmente se denomina **spam** o “correo basura” a todo tipo de comunicación **no solicitada**, realizada por vía electrónica, generalmente emitida de forma masiva.

De este modo se entiende por spam cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada generalmente es mediante el correo electrónico.

Dentro de la definición de correo electrónico, además del servicio de correo electrónico clásico o SMTP (Simple Mail Transfer Protocol), asimismo se incluyen los servicios de mensajes cortos o SMS, mensajes multimedia o MMS, mensajes en contestadores, sistemas de mensajería vocal incluidos en los servicios móviles, y las comunicaciones enviadas desde internet dirigidas directamente a una dirección IP.

El correo electrónico se ha consolidado como uno de los pilares fundamentales de la Sociedad de la Información, cientos de millones de usuarios utilizan en sus ámbitos profesionales y privados esta gran herramienta de comunicación, ya que permite optimizar procesos y aumenta la productividad individual y colectiva. Sus ventajas son múltiples: envía a cualquier parte del mundo y con gran rapidez mensajes a un usuario o grupo de usuarios, permite adjuntar archivos, su coste es bajo, etc. Pero al igual que otros muchos servicios a través de Internet, su utilización casi universal ha sido aprovechada como vehículo masivo de diversas formas de ataques informáticos, a menudo basados en técnicas de ingeniería social (como es el caso del **phishing**, tipo de spam de técnica de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información

bancaria. Es una técnica de intento de fraude ilegal de la que hablaremos con más detalle entre otras más adelante).

Ante las múltiples ventajas que ofrece el correo electrónico podría predecirse que el uso del mismo va a crecer en los próximos años, a medida que aumente la penetración de Internet en la sociedad. Pero, la realidad puede ser otra, y la causa es un importante enemigo que ha surgido para restar eficiencia a esta herramienta: el Spam o correo basura.

En estos momentos el e-mail es objeto de un número cada vez mayor de abusos, hasta el punto de que en la actualidad más del 60% de los correos que circulan por la red son correos basura[1]. Los costes asociados a estos abusos, por ejemplo en el año 2004 y según estimaciones de la OCDE, superaron los 130.000 millones de dólares. Este elevado número de correos basura incide de forma negativa en la confianza de los usuarios y frena el desarrollo de la Sociedad de la Información. Y es que el Spam es la puerta por la que se cuelan más del 90% de las incidencias de seguridad en las empresas y hogares.

Dentro del abanico de usos indebidos de los servicios que presta internet, llama especialmente la atención el auge que está adquiriendo el fenómeno de la recepción de correo no deseado o **spam**, que apareció a finales de los años setenta, con fines generalmente ilegítimos[2].

Internacionalmente el volumen de correo electrónico no deseado o Spam en la Red ha alcanzado en los últimos años proporciones preocupantes. Las cifras concretas de unas y otras fuentes son diversas, pero todas coinciden en el espectacular incremento del Spam en los últimos años. En España en la actualidad el 88% del correo es spam[3] (casi 9 de cada 10 correos).Las razones

[1] COIT(2004)
[2] SPAMINA(2008)
[3] FUNDACION TELEFONICA(2009)

del rápido crecimiento del spam se encuentran en los bajos costes de generación y emisión del mismo, y en la falta de seguridad, así como por la naturaleza internacional de internet, que hace que la legislación no sea igual en todos los países.

La identificación de los países que son mayores generadores de spam, a lo largo de los años ha ido cambiando, según ha ido evolucionando en los países la inclusión de las bandas anchas, adquisiciones de equipos informáticos, cierres de proveedores de alojamiento para remitentes de spam o sobre todo por tener unas leyes menos restrictivas en cuanto a la materia del envío de spam.

En cuanto a los países que son mayores remitentes de spam, en 2008 el volumen analizado por la red de sensores de INTECO indica que entre Estados Unidos, China, Corea del Sur y Rusia envían más del 50% del total de mensajes no deseados o spam que se recibe en España[4].

Atendiendo a cifras en la actualidad, el informe[5] anual emitido en 2011 y que atiende a las cifras estudiadas en 2010, generado por Panda Security, revela que India, Brasil, Vietnam, Rusia y USA son los mayores generadores de spam a nivel mundial.

Aunque generalmente la forma más común de spam es mediante correo electrónico, hay tecnologías de Internet que han sido asimismo objeto de "correo basura" como **grupos de noticias**, **usenet**, **motores de búsqueda**, **redes sociales**, **wikis**, **foros**, **blogs**, también a través de **ventanas emergentes** y todo tipo de **imágenes** y **textos** en la **web**.

El "correo basura" también puede tener como objetivo los **teléfonos móviles** (a través de mensajes de texto o sistemas de mensajería vocal) y los **sistemas de mensajería instantánea** como por ejemplo Outlook, Lotus Notes, etc. y la **telefonía de voz sobre IP** (VoIP).

[4] INTECO(2008)
[5] Panda Security(2011)

Resulta complicado homogeneizar una clasificación de los diferentes tipos de spam por la diversidad de técnicas empleadas por los spammers (responsables del envío de spam), pero se puede agrupar por el contenido del mensaje, por el formato del texto del mensaje o por sus evoluciones, nuevos medios o contenidos (como los de mensajería instantánea o través del teléfono móvil, etc.)[6].

Actualmente existe una importante discusión sobre qué se considera spam, centrada en el marco de los correos masivos de listas de distribución y publicitarios. Han aparecido dos sistemas de control sobre la recepción de este tipo de correos para regularlos: la aceptación previa para la primera comunicación (sistema conocido por **opt-in**) o la opción de cancelación en cada comunicación (sistema **opt-out**)[3].

La catalogación como spam de correos electrónicos legítimos, los llamados falsos positivos, tiene asociado importantes perjuicios para las organizaciones. En el mejor de los casos, es necesario que los usuarios y técnicos del sistema inviertan un tiempo significativo en la recuperación de esos correos legítimos, eso si no ha sido eliminado definitivamente. Las pérdidas monetarias que puede ocasionar la no recepción de esos correos no pueden ser calculadas[7].

Internet no sólo pude ser entendido como una red de comunicación de fácil y eficiente difusión y una fuente inestimable de información. Es además un gran mercado y un poderoso instrumento al servicio de los intereses comerciales de las empresas en orden a la difusión de sus servicios y productos. La mayoría de empresas dispone de página web donde puede anunciar sus servicios o

[6] INTECO(2008)
[7] INTECO(2008)

productos, y la forma de comunicación de las mismas es mediante el uso de correo electrónico frecuentemente por el bajo coste que supone.

Asimismo, las empresas orientan su estrategia de marketing hacia un aprovechamiento e inversión en el uso y conocimiento de los instrumentos de comunicación en línea que operan en internet. El rendimiento que estas empresas pueden obtener por medio de las tecnologías de la información y la comunicación con finalidades comerciales es notable[8].

El informe[9] que recoge los resultados del Observatorio de Marketing Directo e Interactivo revela que el 78% de las empresas anunciantes utilizan herramientas de marketing directo e interactivo de un total de una muestra de 213 empresas seleccionadas entre los 1.030 primeros anunciantes españoles, datos obtenidos de los resultados del Observatorio del Marketing Directo e Interactivo 2009, elaborado por la Asociación de Agencias de Marketing Directo e Interactivo (AGEMDI- Fecemd) y la Asociación de Anunciantes (AEA).

Entre las herramientas de marketing directo e interactivo, una de las más estandarizadas en su uso empresarial para las comunicaciones es el correo electrónico. Y no solo queda en el ámbito empresarial, tanto la Administración como las empresas y los millones de usuarios finales emplean frecuentemente como comunicación electrónica preferida el uso del correo electrónico, con lo cual, este hecho provoca una susceptibilidad mayor a la recepción del correo basura o spam y los problemas asociados que éste provoca:

Pérdidas en tiempo (el tiempo que cada trabajador dedica a eliminar el spam de su buzón de correo está entre dos y cuatro minutos al día por término medio. Este es un hecho que no parece importante, pero sólo por la pérdida de tiempo que supone la eliminación del spam, en el año 2007 el coste económico asociado a cada trabajador que utiliza diariamente el correo electrónico en su puesto de trabajo, se estima en 179€[10]), desconfianza en el servicio, consumos

[8] Álvarez(2010)
[9] Agencias Digitales(2009)
[10] INTECO(2008)

de ancho de banda y en capacidad de almacenamiento, tiempos de recuperación y restablecimiento, necesidad de nuevas inversiones en técnicos especializados, herramientas antispam y nuevas infraestructuras para minimizar la recepción de spam, pérdidas económicas como consecuencia de la pérdida de información relevante para la actividad y otro tipo de problemas de tipo fraudulento e ilegal (phising, scam, spoofing, etc.)[11] que pueden desembocar en hechos económicamente desastrosos.

Aunque resulte sorprendente hay agentes que están claramente a favor de estas prácticas: los que directamente practican el spam, los que crean herramientas y servicios para los spammers, y los que trafican con bases de datos y direcciones. En el otro extremo se encuentran los gobiernos de países industrializados, las empresas y los usuarios que claramente están en contra de estos abusos. Como siempre, hay una zona intermedia en la que podemos ubicar a los que se benefician indirectamente de esta situación: empresas que proveen soluciones y servicios para combatir el spam, y organizaciones de marketing directo que ven en el correo electrónico una gran herramienta de marketing, siempre que se use de forma adecuada[12].

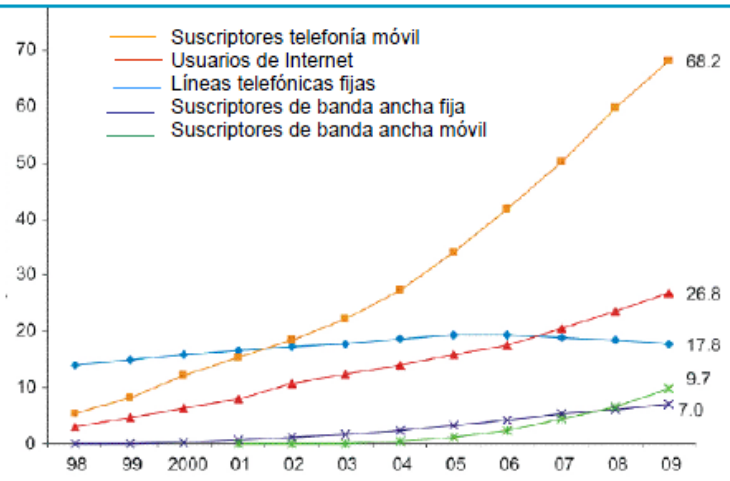
Recordando la definición práctica de spam como cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa, podemos deducir que el spam es un gran negocio que invade nuestros buzones de correo electrónico y con consecuencias ya comentadas.

A lo largo del tiempo, la mejora de los accesos a Internet ha incrementado el volumen del spam tanto por parte de los emisores como destinatarios. Los emisores porque disponen de más posibilidades de ancho de banda y uso de

[11] En el apartado *4.5- tipos de spam* del presente documento se explican estas técnicas de fraude informático y otras importantes.
[12] COIT(2004)

servidores propios. Los receptores porque debido a las tarifa planas y la consecuente reducción del coste de consultar el correo, ya no es tan costoso económicamente (no como en un tiempo anterior a las tarifas planas, en el que el coste era por tiempo de conexión), con lo que la recepción de spam se asume con resignación por parte de la mayoría de los destinatarios. Este hecho lo podemos constatar en la gráfica[13] siguiente en la que podemos observar la evolución a lo largo de los últimos años tanto de los usuarios de internet como de la banda ancha en todo el mundo:

Evolución de la banda ancha móvil y otros indicadores TIC en el mundo



* Datos estimados

Fuente: UIT

El bajo coste de los envíos vía Internet (mediante el correo electrónico) o mediante telefonía móvil (SMS y MMS), su posible anonimato, la velocidad con que llega a los destinatarios y las posibilidades en el volumen de las transmisiones, han permitido que la práctica del spam se realice de forma abusiva e indiscriminada[14].

El spam es un simple reflejo de la actual sociedad donde la publicidad inunda todos los rincones[15]. Los contenidos del spam son variados y difíciles de

[13] ONTSI(2010)
[14] AEPD(2005)
[15] Sanz(2003)

clasificar, pero lo cierto es que generalmente los hay de carácter sobre todo molesto con fines publicitarios o comerciales (la mayoría) y los de carácter fraudulento e ilegal, que pueden ocasionar graves problemas y delitos flagrantes, tanto a particulares como a empresas o incluso a la misma administración pública, siendo vulnerable a esta problemática cualquier entidad o particular que realice comunicaciones electrónicas sobre todo mediante el uso del e-mail o correo electrónico.

Los usuarios indican que el spam es la incidencia más frecuente, por encima incluso de los códigos maliciosos[16] (troyanos, programas espía, etc.), con lo cual se ha generado una desconfianza relativa entre los usuarios habituales del correo electrónico. El grado de desconfianza es mayor en el entorno laboral que en el doméstico, dada la importancia asociada al contenido de los mensajes en cada caso.

Por todo ello, ha habido un cambio en la conducta del usuario ante el correo electrónico como consecuencia del spam, siendo cada vez más frecuente que los usuarios tomen medidas de protección ante la recepción del correo basura como el uso de programas antispam, aunque los usuarios ante la dimensión de esta problemática vienen reclamando medidas formativas y de carácter legislativo que hagan frente al spam con la intención de fortalecer unas medidas normativas inequívocas que esclarezcan las posibles acciones y sanciones correspondientes frente a los responsables del envío del correo basura o spammers.

La naturaleza internacional de Internet y de las direcciones IP origen inhabilita en un principio cualquier medida legal para reducir o sobre todo erradicar el problema del spam a nivel mundial[17].

[16] INTECO(2008)
[17] Sanz(2003)

Ante este panorama se plantean nuevos retos, entre los que cabe destacar el control sobre el uso indiscriminado del correo electrónico para realizar comunicaciones comerciales no solicitadas o fraudulentas, que suponen una clara amenaza para organizaciones y particulares.

Para combatir esta problemática, se han previsto acciones de refuerzo de la seguridad y confianza en la Red dirigidas a ciudadanos, empresas y administraciones públicas, como pasaremos a observar en posteriores apartados del presente proyecto.

3- El correo electrónico no deseado o SPAM

3.1-Historia del término y origen del spam

El origen de la palabra spam tiene raíces estadounidenses. La empresa charcutera estadounidense Hormel Foods lanzó en 1937una carne en lata originalmente llamada Hormel's Spiced Ham. El Spam fue el alimento de los soldados soviéticos y británicos en la Segunda Guerra Mundial y desde 1957 fue comercializado en latas que ahorraban al consumidor el uso del abrelatas.

Más adelante, el grupo británico Monty Python empezó a hacer burla de la carne en lata. Su costumbre de gritar la palabra spam en diversos anuncios publicitarios se trasladó al correo electrónico no solicitado, también llamado correo basura.

Aunque existen otras versiones de su origen los orígenes del spam se datan el 3 de mayo de 1978. El primer mensaje reconocido como tal fue enviado a los 393 empleados de ARPANET[18] en mayo de 1978. El creador de este correo fue Gary Thuerk, un comercial de DEC (Digital Equipment Corporation), que envió

[18] ARPANET (Advanced Research Projects Agency Network) fue creada por encargo del Departamento de Defensa de los Estados Unidos como medio de comunicación para los diferentes organismos del país y está considerada la red que dio origen a Internet.

un mensaje publicitario a una lista de usuarios ARPANET, sobre los que su empresa deseaba ampliar mercado, invitándoles al lanzamiento de un nuevo producto. Dicha invitación fue hecha manualmente. Aunque la información enviada resultó de interés para alguno de los destinatarios, los problemas que ocasionó en el sistema iniciaron el debate sobre la conveniencia o no de controlar el correo y, de algún modo, censurar aquellos publicitarios de envío masivo.

En 1994, los abogados Canter y Martha SIegel de Phoenix enviaron correos masivos publicitando exitosamente su firma, quedando así al descubierto las ventajas del uso de esta vía y la enorme influencia que tenía sobre los cada vez más usuarios de la red global. Pero al tiempo que se abría esta puerta en beneficio de los negocios, se abrían otras muchas que no sólo favorecían el crecimiento del envío y reenvío incontrolado de estos mensajes no deseados, sino además otras amenazas de seguridad, como los códigos maliciosos (troyanos, spyware, etc.) o el phishing, quedando al descubierto las potenciales ventajas de tal práctica frente al número considerable de desventajas que la misma podía provocar.

3.2- Definición de spam

Destacan dos definiciones del término, hasta el momento las más citadas, que aparecen publicadas en el proyecto Spamhaus[19], dedicado a la protección en tiempo real del spam:

-La primera denomina spam al "correo electrónico masivo no deseado" (en inglés UBE, Unsolicited Bulk E- Mail).

-La segunda lo define como todos aquellos correos publicitarios no autorizados (en inglés UCE, Unsolicited Comercial E-Mail).

[19] http://www.spamhaus.org

Una definición más formal, en términos de políticas de empleo aceptable del correo, es dada por Mail Abuse Prevention System[20], por la que el correo electrónico debe ser considerado spam si cumple las siguientes condiciones:

-La identidad del destinatario del correo y el contenido son irrelevantes, por cuanto el mensaje no está personalizado y podría aplicarse a muchos otros receptores.

-El destinatario no ha concedido permiso para que se le envíe el mensaje.

-La recepción del mensaje brinda un beneficio al que lo recibe.

Finalmente atendiendo a la definición[21] que presta la Agencia Española de Protección de Datos (AEPD), actualmente se denomina Spam o "correo basura" a todo tipo de comunicación **no solicitada**, realizada por vía electrónica.

De este modo se entiende por Spam cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico.

Esta definición es matizada por la Comunicación, de 22/01/2004, de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones comerciales no solicitadas o spam:

"*El término spam suele usarse para designar el envío, a menudo* ***masivo****, de mensajes electrónicos no solicitados. La nueva Directiva no define el término spam ni lo utiliza. Recurre a los conceptos de «comunicaciones no solicitadas» transmitidas por «correo electrónico» «con fines de venta directa» que, conjuntamente, cubren de hecho la mayoría de los tipos de spam. El concepto de*

[20] Mail Abuse Prevention System (MAPS): Asociación internacional de lucha contra el *spam*. http://www.mail-abuse.com

[21] AEPD (2005)

spam se utiliza, pues, en la presente Comunicación como sinónimo de «correo electrónico comercial no solicitado».

Conviene observar que el concepto de «correo electrónico» cubre no sólo los mensajes electrónicos tradicionales que utilizan el protocolo SMTP, sino también los SMS, los MMS y cualquier forma de comunicación electrónica en la que no se requiera la participación simultánea del remitente y el destinatario."

Queda matizada la definición de spam que aporta la AEPD, aportando el carácter de masividad al envío de los correos electrónicos no solicitados. Con lo cual se puede considerar spam a los mensajes electrónicos no solicitados enviados en cantidades masivas a un número muy amplio de usuarios.

Relativo a este punto cabe señalar que el envío de spam es particularmente grave cuando se realiza en forma masiva.

3.3- Generación y distribución del spam

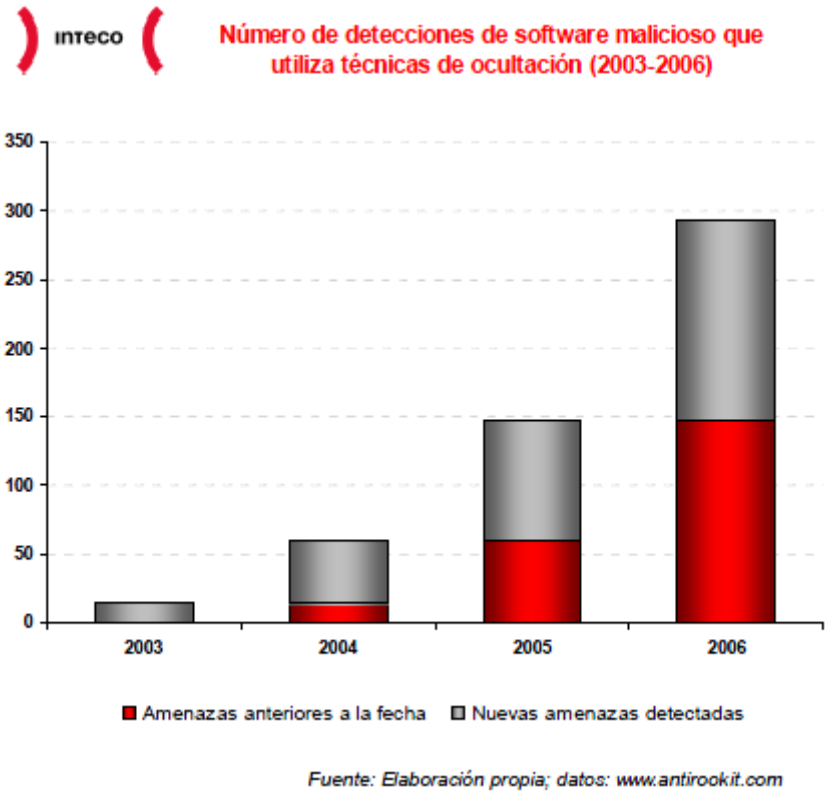
Los spammers son los responsables de desarrollar y/o desplegar el correo de tipo spam, ya sea de forma particular u organizada con fines lucrativos.

Se denomina spamware[22] al software desarrollado por los spammers para la generación y envío de spam. Así, el spamware puede incorporar, conjunta o separadamente, funcionalidades para la obtención o creación de direcciones de correo objetivos, el envío y distribución masiva de forma automática de e-mails o la explotación de vulnerabilidades de los sistemas. La intención de este software maligno es la de conseguir el máximo de direcciones de correo objetivo de los envíos de spam, así como su envío automático a estas direcciones de los correos basura (spam), pudiendo acceder a tales direcciones explorando las debilidades existentes en los sistemas para su posterior intrusión en ellos, recopilando la información deseada, en forma de listas de direcciones de correo electrónico que serán los potenciales destinos de los envíos de spam,

[22] INTECO(2008)

o en el peor de los casos, pudiendo obtener datos confidenciales con el peligro que ello comporta.

Hay que resaltar que el spamware, es un tipo de software malicioso que utiliza técnicas de ocultación, para que el usuario del PC infectado no se percate de lo que verdaderamente está ocurriendo en su ordenador. Este tipo de software ha ido incrementando a lo largo de los años como podemos ver en la siguiente gráfica[23]:



Aunque muchos de los correos basura son eliminados por los receptores en los buzones de destino sin llegar a ser abiertos, hay otros que son reenviados por diversos motivos como tras leer un correo interesante, sensacionalista o aparentemente ventajoso. En este caso los destinatarios deciden reenviárselo a sus conocidos, expandiendo las direcciones objetivo del spam, o en el peor de

[23] INTECO(2007a)

los casos, realizar otras acciones a las que el propio contenido del correo les induce (por ejemplo, ejecutar un fichero adjunto, visitar un determinado sitio web o hacer una compra online), acciones que pueden ser susceptibles de intentos de fraude o que pueden contaminar nuestro ordenador con un virus con el propósito de conseguir más direcciones objetivo destino e incluso hacer que nuestro PC distribuya spam automáticamente a tales direcciones, además de la posibilidad del robo de datos confidenciales o utilizar los recursos del ordenador infectado. Por ello, el spam forma parte de las amenazas de seguridad que recurren a la ingeniería social.

Continuamente se están desarrollando diversas técnicas y medidas contra el spam (antispam), pero paralelamente, los spammers estudian estas variantes para generar nuevas formas que mejoren las anteriores y consigan burlar la actuación de las herramientas antispam. Incluso en muchos casos se aprovechan precisamente de su existencia para generar nuevos problemas en las comunicaciones y en los sistemas: por ejemplo, la aparición de falsos positivos, correos electrónicos válidos que son filtrados por el software antispam como correo electrónico no deseado cuando no lo son. Ante esto, muchos usuarios solicitan a su administrador del servicio de correo la desactivación de dicha protección ante el riesgo de perder correos importantes, favoreciendo así la actividad de los spammers[24].

Una de las características actuales en el envío del spam consiste en la utilización de las botnets o redes de ordenadores comprometidos como plataforma para el envío de los correos y ocultación del rastro del spammer. Son redes en las que los spammers instalan un software específico que les permite controlar y utilizar las máquinas a través de Internet para sus fines. Cada uno de

[24] INTECO(2008)

estos ordenadores suele conocerse con el nombre de máquina zombie, y está bajo el control total del atacante[25].

Una vez que un ordenador ha sido contagiado, normalmente a través de un troyano, entra a formar parte automáticamente de la botnet (red de ordenadores comprometidos), quedando a la espera de instrucciones que le dará el spammer, tradicionalmente a través de canales de Chat IRC, aunque últimamente hacen uso de las redes P2P[26] para ser más eficientes. Cada uno de los ordenadores de esta red botnet funciona con aparente normalidad para cada uno de sus usuarios, permitiendo a un intruso tomar el control de un ordenador sin que el usuario lo advierta, con el consiguiente peligro que ello supone, ya que además de la instalación de un bot en el ordenador contagiado, puede haber un robo de datos sensibles de los usuarios como datos confidenciales (bancarios, correspondencia, contraseñas, etc.), todo ello sin que el usuario se percate. Aparte de esta problemática potencialmente grave, dicho control permite al intruso utilizar los recursos del ordenador huésped, bien para ocupar parte de su ancho de banda para la descarga de contenidos de gran tamaño o bien para almacenar archivos en su memoria.

Para la captación de nuevos ordenadores comprometidos, existen tres vías fundamentales para que los atacantes consigan añadir nuestro PC a la red botnet[27]: por navegación web (navegar por Internet puede producir que una máquina sea comprometida, habitualmente aprovechando vulnerabilidades en los navegadores), a través de redes P2P (en este tipo de redes no existen mecanismos de seguridad integrados. Según algunos estudios recientes, casi el 50% de los programas ejecutables que pueden encontrarse en estas redes están infectados con alguna clase de malware, que es software de carácter

[25] INTECO(2007a)
[26] *Peer-to-peer*: red que no tiene clientes ni servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la Red.
[27] INTECO(2008)

malicioso), y finalmente a través del correo electrónico (el malware se camufla como un programa legítimo como por ejemplo salvapantallas, juegos, etc.).

Resumiendo, el objetivo final de esta "red de ordenadores zombis" es su utilización para el envío masivo de correo basura (spam), el ataque a otros sistemas, las estafas por Internet (phishing), la captura de datos confidenciales, o la realización de un ataque mediante el envío masivo y coordinado de un volumen de información tal que se sobrecarguen y colapsen los sistemas informáticos o las páginas web de organismos y empresas (técnicamente conocido como un DDoS o ataque de denegación de servicio distribuido).

Cabe resaltar que existe un mercado ilegal creciente donde pueden contratarse los servicios de estas redes para el envío masivo de publicidad no deseada o para realizar dichos ataques de denegación de servicio.

El spamware no es muy diferente a otros tipos de malware, por lo que las medidas para evitar que el ordenador entre a formar parte de una red son también similares. El estudio[28] de INTECO acerca del spam nos recomienda a modo de resumen las siguientes acciones: bloquear todo el tráfico de correo entrante no solicitado en los cortafuegos perimetrales, utilizar herramientas antivirus actualizadas, actualizar el sistema de los equipos (descargar los parches de actualización de programas o del sistema operativo para mejorar la vulnerabilidad del PC), o bloquear del tráfico de salida en el puerto 25 (SMTP).

[28] INTECO(2008)

3.4- Ciclo de vida del spam

El spam se desarrolla en diferentes etapas, como indica el estudio[29] realizado por INTECO. Básicamente son las relacionadas con la búsqueda de los puntos de entrada al sistema, es decir, con la recolección de direcciones de correo electrónico. A continuación, se produce la creación del correo spam, seguida del envío y ataque y, por último, la comprobación de su éxito y el refinamiento de las listas empleadas. A continuación, pasamos a identificar y describir brevemente las fases del ciclo de desarrollo del spam:

- Fase I: **recolección de direcciones de correo**: recopilan o generan automáticamente direcciones de correo activas (en uso) a las que se enviará el spam. La recopilación de direcciones puede obtenerse de páginas web, de listas de correo o mediante ingeniería social (como los reenvíos de e-mails en cadena, que permiten obtener el listado de direcciones a las que se envió dicho correo en el momento que vuelve a llegar el mismo mail al spammer).

La generación automática de las direcciones se realiza mediante técnicas más sofisticadas como el uso de robots de búsquedas, el ataque a servidores de correos o PC (técnica hacker que entra ilícitamente en los ordenadores personales o incluso servidores de correo, obteniendo los listados deseados), ataque a aplicaciones de Internet (las más usuales aprovechan vulnerabilidades del navegador web), mediante búsqueda por diccionario (se generan las listas aleatoriamente y se comprueba si las direcciones existen y están activas), o mediante la solicitud directa de la dirección de correo mediante páginas web engañosas que piden la dirección de correo para acceder al servicio ofertado.

Hay que destacar que existe otro método de obtención de dichas listas de direcciones: mediante la compra directa de bases de datos de direcciones de correo, método que es fraudulento e ilegal en la mayor parte de los países.

[29] INTECO(2008)

- Fase II: **creación del correo spam**: Se genera un mensaje de correo que llame la atención al receptor para que decida leerlo e induzca al destinatario a responderlo, reenviarlo o realizar cualquier otra acción requerida. Todo ello lo hará de forma creíble que no induzca a pensar al destinatario que se trata de spam, por ejemplo simulando que se remite ese correo por una solicitación previa de información por parte del usuario. Cabe destacar que las acciones que son requeridas en el correo spam, vienen en forma de datos de contactos como números de teléfono, dirección de correo o enlaces web, o incluir directamente hipervínculos. Esta parte constituye el elemento fundamental del correo spam, pues es la que define su objetivo y ataque. Aquí puede combinarse con otros ataques como los de phishing, inyección de virus, troyanos, etcétera. Asimismo existen correos de spam que incluso ofrecen la posibilidad de no continuar recibiendo este tipo de mensajes (opción opt-out), pero a diferencia de los correos publicitarios lícitos, en los falsos esta opción persigue el objetivo de hacerlo más creíble y puede tratarse de una forma de desplegar un determinado ataque (por ejemplo, nos remite a un enlace web para dar de baja la recepción de estos correos, donde puede darse un ataque como los mencionados en el anterior párrafo) o simplemente de comprobar que la dirección de correo a la que se envió el correo basura se encuentra activa para permanecer en las listas de distribución de los spammers.

-Fase III: **envío masivo del spam**: Es el momento en el cual el spammer elige y desarrolla diversas técnicas de envío del mensaje de correo para que llegue a sus múltiples destinos, evitando las posibles protecciones y ser descubierto como emisor del mensaje. Una vez realizado el reenvío continuado, se podrán desplegar ciertos ataques en cada máquina, a menudo con la colaboración involuntaria del usuario.

Normalmente el envío de spam se hace de forma automática y masiva mediante diferentes técnicas como las basadas en servidores de correo con

configuración abierta (estos servidores no necesitan usuario y contraseña para enviar e-mails, con lo que el spammer no necesita ser cliente del servidor y puede evitar ser identificado), técnicas basadas en troyanos spammers (son perfectas para los spammers ya que permiten infectar y tomar el control de miles de computadores en Internet, utilizándolas como plataformas de envío de spam, gastando sus recursos o captando los datos comprometidos de los usuarios de dichas máquinas infectadas), técnicas basadas en servidores SMTP internos (las herramientas de envío de spam incorporan un motor de envío de mensajes SMTP para enviar automáticamente el correo sin tener que conectarse a un servidor externo, con la intención de sortear las listas negras de servidores. Se combina generalmente con los troyanos spammers), o las técnicas basabas en redes de ordenadores comprometidos (resultado de la infección mediante la técnica de troyanos spammers de un gran número de computadores que remitirán spam. El malware instalado en las mismas, permite este envío automático de spam incluso a las direcciones almacenadas en el PC comprometido, pudiendo hacer uso del servidor externo de correo del cual es cliente el usuario de estos PCs).

Las técnicas de envío masivo de mensajes de correo suelen combinarse con ciertas técnicas de tratamiento de los mensajes que dificultan aún más su detección y rastreo, como las técnicas basadas en el falseo del remitente (enviar un correo a nombre de un emisor falso con la intención básicamente de comprobar que la dirección destino está activa), las basadas en la personalización de los mensajes (emplear un mensaje como plantilla general y adaptarlo con datos específicos de cada destinatario mediante información recolectada en Internet o extraída de la propia dirección de correo), y por último las técnicas basadas en la ofuscación del mensaje (ocultan automáticamente el texto del mensaje con la intención de que sea difícil de detectar y rastrear por parte de los filtros antispam). Hay varias técnicas de ofuscación como mediante imágenes (el mensaje spam va incrustado en una

imagen y no un texto), mediante invisibilidad del texto (ocultan el mensaje spam dentro de un texto legítimo, mediante letras espaciadas que introducen caracteres o espacios blancos entre las letras del mensaje spam), mediante corte vertical (ocultan el texto en una tabla HTML), o mediante código script (en vez de enviar el contenido spam en texto, envía un script que lo genera y que interpreta la aplicación cliente como el navegador, etc.).

Hay que resaltar que no suelen emplearse medidas de autenticación en los protocolos de envío de correo electrónico, con lo cual no hay una autenticación del remitente. Esto se traduce en que cualquier individuo u organización puede poner en marcha un servidor de correo y enviar y recibir un número ilimitado de correos electrónicos.

-Fase IV: **refinamiento de listas**: Mecanismo para comprobar la existencia y el estado activo de las direcciones de correo a los que se envía el spam, con el fin de eliminar direcciones de correo desactivadas o inexistentes, para aumentar el número de contactos válidos.

Las técnicas más usadas para tal fin son las pruebas de lectura (al leer o previsualizar el spam, el spammer puede comprobar quién, cuándo y desde qué ordenador se leyó dicho mail, corroborando el uso activo de tal dirección de correo), enlaces y páginas para darse de baja en listas (el spam recibido contiene un enlace para, supuestamente, tramitar la baja de la dirección en las listas de suscripción, pero dicha baja no sólo no se produce, sino que aumenta del volumen de spam recibido ya que al solicitar la baja, se está confirmando que la dirección es válida y queda incluida en nuevas listas de spammers), y por último correos de confirmación (spam ilegítimo que engaña al usuario pidiendo al mismo que responda al correo, sin proporcionar datos, o bien le indique que su silencio se tomará como una aceptación a estar en la lista de distribución, con lo que si se responde, se comprueba el estado activo de su dirección de correo, pasando a las nuevas listas de spammers).

A modo de resumen de las fases del ciclo de vida del spam, se incluye la siguiente tabla elaborada por INTECO en su estudio[30]:

Es muy importante destacar que en general, no es aconsejable seguir **ningún** enlace incluido en un spam, pues, habitualmente, apuntará a páginas que

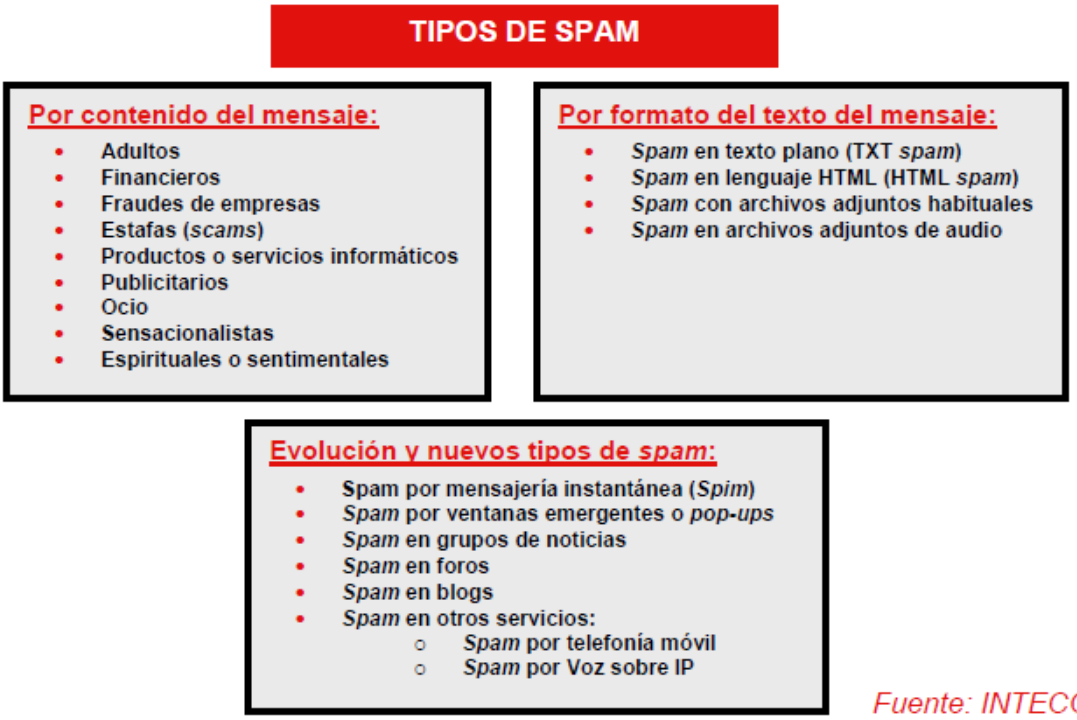
[30] INTECO(2008)

contienen troyanos spammers u otro tipo de malware. Los diferentes motivos se explican en este último apartado.

3.5- Tipos de spam

La clasificación de los diferentes tipos de spam es complicada, pues las técnicas empleadas por los spammers son cada vez más ingeniosas y sofisticadas y suelen ser cambiantes a la par que se evoluciona en los mecanismos que intentan ponerle freno. A continuación se proponen dos clasificaciones:

La primera clasificación es la elaborada por el estudio[31] de INTECO respecto a la materia. Esta clasificación tiene una intención ilustrativa y no limitativa de los distintos tipos de correo no deseado que está basada en la clasificación realizada por Symantec Corporation[32]. Por su gran extensión se resume en la siguiente tabla extraída del citado estudio, ya que sus aspectos más importantes están incluidos en la segunda clasificación propuesta:



Fuente: INTECO

[31] INTECO(2008)
[32] http://www.symantec.com/

Simplemente destacar en la clasificación por el contenido del mensaje que el tipo de spam “Fraudes a empresas” se corresponde con el conocido **phishing** (técnica de ingeniería social por la cual un atacante intenta adquirir información confidencial de una víctima de forma fraudulenta, haciéndose pasar por un tercero de confianza) o **brand spoofing** (similar al anterior, es una técnica de suplantación de identidad de la marca de una empresa imitada). Puede estar asimismo clasificado dentro de la clase de estafas (**scams**). Asimismo existe genéricamente el **spoofing** (suplantación de identidad o personalidad. Suplanta a la persona con la identificación de sus datos sensibles y confidenciales que consiguió por ejemplo mediante **phising**). Atenderemos con más detalle a estas técnicas y otras en la siguiente clasificación propuesta. Asimismo resaltar que los destinos de los correos basura no se limitan al correo electrónico, sino que hay nuevas formas de spam que se han extendido a nuevos objetivos destino como en la **mensajería instantánea** (ICQ, Messenger o Skype, etc.), **por ventanas emergentes o pop-ups** (al navegar por internet), en **grupos de noticias**, en **foros**, en **blogs**, incluso se llegan a extender a la **telefonía móvil** (a través de **SMS** o **MMS**) y a las **comunicaciones VoIP** mediante mensajes pregrabados. Y no se limita ahí, ya que aunque no sea definido como spam, sufrimos fenómenos parecidos en nuestra vida cotidiana a través de sistemas como el fax y el teléfono tradicional, en sistemas automáticos de envío y recepción de llamadas, puerta a puerta, a través de folletos y otras promociones que llegan a los hogares o empresas, etc.

Asimismo es interesante destacar dentro de la clasificación por el formato del texto del mensaje spam sus distintos tipos:

-Spam **en texto plano** (TXT spam): es el formato más común en el cuerpo del mensaje de los correos electrónicos. Es una de las técnicas más utilizadas por su sencillez, pero también es el más fácil de detectar por los filtros antispam. Utiliza principalmente técnicas de ingeniería social para persuadir a los

receptores y desplegar su ataque o ser nuevamente enviado (mensajes en cadena).

-Spam **en lenguaje HTML** (HTML spam): el contenido del mensaje es un fichero HTML[33] que la mayoría de los clientes de correo permiten visualizar directamente. Este tipo de mensaje, por las propiedades de los ficheros HTML, permite incluir código y técnicas automatizadas para realizar sus acciones y ser reenviados.

- Spam **con archivos adjuntos habituales**: el contenido de tipo spam no es enviado en el cuerpo del mensaje, sino en un fichero adjunto. Antiguamente los ficheros adjuntos tenían extensiones .ppt o .zip, pero en la actualidad se está extendiendo el uso del *spam* a imágenes y archivos .pdf.

-Spam **en archivos adjuntos de audio**: es la tendencia más reciente en técnicas spammers. Consiste en enviar mensajes codificados en archivos adjuntos de audio MP3 de pocos segundos, grabado a un bajo nivel de bits y con una voz sintetizada (para evitar los filtros antispam por búsqueda de patrones de voz) que promociona un determinado producto.

La segunda clasificación propuesta es la elaborada por otro estudio[34] de INTECO que parte de la utilizada por la propia Agencia Española de Protección de Datos, relativa a finalidad que persigue el correo spam:

- Spam **con fines comerciales**: se trata del pionero, y tiene como objetivo difundir la utilidad de un producto o la posibilidad de adquirirlo a un precio inferior al de mercado. En algunos casos, tiene relación con algunos tipos delictivos, ya que en la actualidad se están ofertando por este método productos que infringen las leyes de propiedad intelectual, de patentes o normativas sanitarias (por ejemplo se ofrecen medicamentos, relojes y joyas, música, etc.).

[33] *HyperText Markup Language*,. Es un lenguaje diseñado para estructurar textos y presentarlos en forma de hipertexto en las páginas web.
[34] INTECO(2007)

-El **bulo** (**hoax**): mensaje de correo electrónico con contenido falso o engañoso, generalmente enviados en cadena y que solicita al receptor reenvíos posteriores continuando dicha cadena. En ellos se cuenta una historia más o menos verosímil relativa a injusticias, abusos, problemas sociales o temas interesantes para el receptor, con el fin de captar direcciones de correo electrónico (que se van acumulando en el proceso de reenvío) que serán utilizadas posteriormente como destino de spam. Existe un problema con su regulación legal, ya que no constituye en sí mismo una infracción de la ley, al no tratarse de comunicaciones comerciales.

-El spam **con fines fraudulentos**: el spam puede ser, en muchos casos, la catapulta para la comisión de un fraude. La mayoría de los intentos de fraude (**phishing**, las clásicas "cartas nigerianas"[35], **scam** y otras modalidades fraudulentas) llegan a sus destinatarios a través de su correo electrónico.

-Spam **con otros fines delictivos**: a medio camino entre el bulo (**hoax**) y el fraude (**scam**, **phising**, **spoofing**, etc.). A través de un ataque de spamming se puede tratar de dañar la reputación de una persona física o jurídica, propagando rumores de poca certeza que vienen remitidos por contactos conocidos.

También es interesante señalar un malware de tipo publicitario que puede introducirse en nuestro equipo con fines de envío de spam personalizado al usuario y que últimamente está en auge, este es el **Adware o software publicitario**: muestra anuncios publicitarios que aparecen inesperadamente en el equipo cuando se está utilizando la conexión a una página web o después de instalase en la memoria de la computadora. En ocasiones recopilan información sobre los hábitos de navegación de los usuarios para luego redirigirles a la publicidad coincidente con sus intereses. El Adware tiene una incidencia del

[35] Se ofrece un negocio fácil y con suculentos beneficios y se solicita a la victima un anticipo económico para afrontar los gastos iniciales.

34.4% de los equipos de los usuarios, a fecha del 2009 según un estudio[36] de INTECO.

3.6- Impacto económico y social del spam

En referencia al impacto económico, conviene destacar la ausencia de información fidedigna o de estudios detallados que permitan arrojar cifras fiables. El cálculo preciso de las pérdidas generadas por el spam, es muy dificultoso. Existen muchas variables implicadas en el proceso del *spam* que generan un marco de complejo análisis. Entre ellas se pueden encontrar los rápidos avances que se producen en la seguridad de la información, como las mejoras en los filtros antispam de los servidores de correo que no permiten un seguimiento homogéneo, o el hecho de que no todas las empresas tienen dichos filtros instalados en sus servidores. El cálculo también se complica por las diferentes cifras que se manejan sobre volumen de spam en circulación. A todo esto se añade que el coste laboral para la empresa, de cada uno de sus trabajadores, no es el mismo según el puesto que ocupen, lo que provoca realizar nuevas estimaciones sobre dicho dato. Y finalmente definir el impacto del número de trabajadores afectados que, ya no sólo utilizan el ordenador en su puesto de trabajo, sino que hacen uso frecuente del correo electrónico como herramienta de trabajo. Todo ello determina que en los cálculos sobre impacto económico se hable siempre de estimaciones basadas en predicciones estadísticas[37].

Los análisis sobre las consecuencias del spam en organizaciones y usuarios se identifican claramente sobre los efectos derivados del mismo: pérdidas de tiempo y productividad (de los procesos y de los usuarios), desconfianza en el servicio (los proveedores de servicio de correo, deben invertir en infraestructuras primarias y de respaldo, en medidas de protección, etc. para

[36] INTECO(2009)
[37] INTECO(2008)

ofrecer un servicio confiable, garantizando la seguridad y disponibilidad del servicio frente a la amenaza del spam. La insatisfacción de los clientes puede llevar a darse de baja del servicio), consumos de ancho de banda y de capacidad de almacenamiento (los spammers utilizan las maquinas contaminadas para su uso en forma de descargas, almacenamientos en disco, generación y distribución de spam, o por el gran volumen de mensajes que provoca una saturación del servidor de correo, etc.), necesidad de un tiempo de recuperación y reestablecimiento del servicio (por ejemplo en ataques de denegación de servicio distribuido o DDoS, al saturar los sistemas), gastos económicos para la necesaria inversión en nuevas infraestructuras tecnológicas (para combatir el spam y sus problemas asociados), gastos por contratación de técnicos cualificados e inversión en herramientas antispam y sus actualizaciones, pérdidas económicas como consecuencia de la pérdida de información relevante para la actividad (puede haber robo de datos importantes al infectarse el PC con un troyano spammer, o simplemente incluso sobrepasando la capacidad del buzón de entrada del usuario se puede perder el correo deseado y útil) y posibles pérdidas económicas por estafas que puede provocar el spam en forma de phising, brand spoofing, scams u otras técnicas fraudulentas.

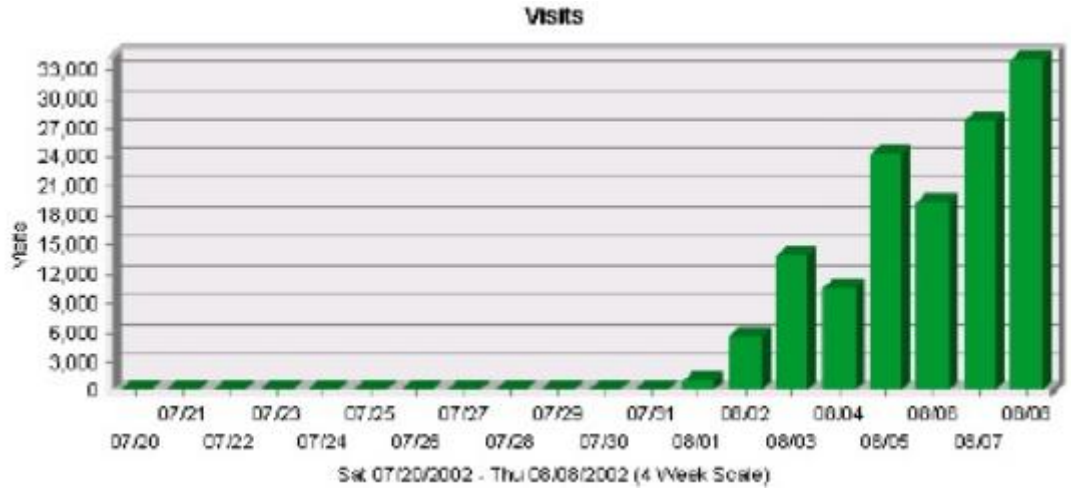
Respecto a los efectos económicos del spam, no se puede obviar que puede consistir en sí mismo en un negocio. Por lo tanto, puede llegar a tener una repercusión económica positiva para aquellas empresas que utilizan el correo masivo como medio de publicidad de sus servicios, sin olvidar a los spammers, que hacen de esta técnica su propio negocio, además de los creadores de herramientas y servicios para los spammers y los traficantes de bases de datos y direcciones . Es importante señalar asimismo en este sentido, que hay un sector que sale beneficiado de los problemas que genera el spam, aunque no tienen parte de responsabilidad en la generación de esta problemática: las

empresas que proveen soluciones y servicios para combatir el spam. Otros beneficiados del spam son las organizaciones de marketing directo que ven en el correo electrónico una gran herramienta de marketing, siempre que la usen de forma adecuada y acorde con la legislación vigente, que se pasa a detallar en los siguientes puntos del proyecto, elaborando finalmente una guía práctica para el cumplimiento de la legislación española y europea en materia de spam.

Para hacernos una idea de los beneficios que puede reportar la generación de spam, en una entrevista[38] a un spammer holandés, el mismo detalla el gasto que le supuso enviar correos masivos durante 25 días y su ganancia neta en ese tiempo que fue de entre 2.000 y 3.000 euros. Y es que la facilidad para enviar spam frente a los potenciales beneficios anima a algunos a convertirse en spammers. La motivación de un beneficio portencialmente alto y rápido les anima a crear sus propias botnets[39].

Para poder apreciar los posibles beneficios a empresas que contratan servicios de spammers, en el siguiente gráfico[40] se muestra cómo es de rentable promocionarse mediantes spam para cierto tipo de negocios. En el gráfico se aprecia la evolución de visitas que experimentó un sitioweb anónimo dedicado a la pornografía, tras promocionarse mediantespam.

[38] https://rejo.zenger.nl/abuse/1085493870.php
[39] INTECO(2008)
[40] El 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.



Fuente: UEFF ("United Email Freedom Front")

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

Hay que destacar que estas cifras no están soportadas por estudios objetivos (no como los cálculos que pasaremos a ver a continuación que sí están contrastados y son verificables, en relación al sobrecoste inducido por la recepción de spam en organizaciones y países), sino por testimonios y entrevistas a spammers, por lo que se advierte que estos datos sólo deben tomarse a modo de curiosidad.

El spam no es sólo un problema de las empresas proveedoras de servicio de correo electrónico, sino que su repercusión llega a todas aquellas organizaciones que hacen uso del servicio de correo. El análisis del impacto económico del spam se fundamenta principalmente en las pérdidas económicas que genera éste en términos de la productividad del empleado. Aunque también resulta difícil su estimación. Sin embargo se pueden establecer algunas estimaciones, calculando el tiempo que este invierte diariamente en

discriminar, de entre todos los correos recibidos, aquellos legítimos que interesan a la organización.[41]

Las pérdidas de productividad por empleado, para aquellos que utilizan habitualmente el correo electrónico pueden calcularse de la siguiente manera[42]: Pérdidas de productividad por cada empleado que usa el correo electrónico =

$$d_T * \left(\sum_{i=1}^{n_{CORREO}} t_{Ei,d,spam} * c_{Ei,h} \right)$$

Donde:

E_i : Representa a un empleado.

d_T : Días de trabajo, por año, de un empleado E_i

n_{CORREO}: Números de empleados que usan el correo.

$t_{Ei,d,spam}$: Tiempo promedio, en horas y por días, que el empleado E_i invierte en gestionar el *spam* de su buzón.

$c_{Ei,h}$: Promedio del coste horario del empleado E_i

Para hacernos una idea de estos valores, en estudios realizados por el Swiss Federal Institute of Technology de Zurich (ETH Zurich[43]), en el año 2005 se estimó una pérdida de productividad de las empresas suizas a consecuencia del spam, **con un coste económico de aproximadamente 2.220 millones de euros**, a partir de los datos que se reflejan en la siguiente tabla[44]:

[41] INTECO(2008)
[42] Dabendofer(2005)
[43] http://www.ethz.ch/
[44] INTECO(2008)

Tabla 2: Impacto económico del *spam* en Suiza (2005)

Factores	Valor
Total de empleados (n_{CORREO})	3.590.000
Días de trabajo, por año, de un empleado (d_T)	230 días
Horas de trabajo, por año, de un empleado	1.880 h/año
Coste medio anual por empleado	63.278 EUR
Coste medio diario por empleado	274,97 EUR
Coste medio por horas de un empleado ($c_{Ei,h}$)	33,66 EUR
En concepto de *spam* el empleado gastaba diariamente ($t_{Ei,d,spam}$)	0,08 h (5 minutos/día)
Pérdida económica diaria asociada al spam por empleado	2,7 €/día
Pérdida económica anual asociada al spam por empleado	621 €/año
Pérdidas de productividad anual por el *spam*	2.220 millones €/año

Fuente: ETH Zurich

A modo de otro ejemplo de impacto todavía mayor, son otras estimaciones realizadas en empresas estadounidenses[45] aun más preocupantes, dado el alto nivel de spam que soporta EE.UU.: ya en el año 2003 señalaban que el spam estaba provocando **pérdidas anuales de 10.000 millones de dólares**. Ese mismo año se publicaron estimaciones de **pérdidas en el mundo cercanas a los 20.500 millones de dólares**[46]. Estos datos han ido con certeza en aumento en los últimos años, debido al incremento significativo del fenómeno spam, como podemos apreciar en el siguiente párrafo.

Atendiendo a otro estudio más reciente del año 2007, "s*pam, the repeat offender*" de Nucleus Research[47] estima que, en la actualidad, los empleados de empresas de Estados Unidos invierten un 1,2% de su tiempo, aproximadamente 5,7 minutos diarios, en identificar los correos electrónicos de spam, generando así un **coste medio de 712 dólares anuales por empleado en concepto de pérdida de productividad**, lo que implica unas **pérdidas anuales de 70.000**

[45] Ferris Research: http://www.ferris.com/
[46] Radicati Group: http://www.radicati.com. Datos extraídos de artículo publicado en el *New York Times* http://www.nytimes.com/2003/07/28/technology/28SPAM.html?ex=1374811200&en=6550b1fd9c0ce99e&ei=5007&partner=USERLAND
[47] Nucleus Research: extraído de "*Spam, the repeat offender*", Report H22, Notes and Reports, abril de 2007. http://nucleusresearch.com/research/notes-and-reports/*spam*-the-repeat-offender

millones de dólares para un total aproximado de 100 millones de empleados que utilizan el correo electrónico. Aunque según estas estadísticas se produjo una mejora considerable en el año 2007 con respecto a 2004, cuando el empleado desperdiciaba el 3,1% de su tiempo reportando un gasto de 1.934 dólares anuales, señalan que no debe considerarse un triunfo, pues las pérdidas continúan siendo considerables y se ha detectado un incremento de falsos positivos en las soluciones antispam. De esta forma, se pierde un número apreciable de correos válidos para la empresa, cuya pérdida económica resulta realmente difícil de estimar. Las tasas de error de las herramientas de protección contra el spam, han generado un cierto rechazo hacia ellas. Podemos apreciar dichas cifras en esta tabla[48] resumen:

Tabla 3: Impacto económico del *spam* en EEUU (2007)

Factores	Valor
Total de empleados (n_{CORREO})	100.249.046
En concepto de *spam* el empleado gastaba diariamente ($t_{Ei,d,spam}$)	5,7 minutos
Pérdida económica asociada al *spam* por empleado	712 USD
Pérdidas de productividad anual por el *spam*	70.000 millones USD

Fuente: Nucleus Research

Las fuentes internacionales señalan en su mayoría que el tiempo medio para eliminar el spam del buzón de correo de un trabajador está entre 3 y aproximadamente 10 minutos diarios[49].

Atendiendo a las cifras en España, el impacto económico del spam en las empresas españolas no es mucho más alentador, según la Agencia Española de Protección de Datos, en datos del año 2005, cada trabajador español necesitaba una media entre 15 y 20 minutos diarios para eliminar el spam de su buzón, es decir aproximadamente un 3,64% de su jornada laboral.

[48] INTECO(2008)
[49] INTECO(2008)

Los datos recabados por INTECO en el estudio[50] sobre la materia, según expertos consultados, apuntan que el tiempo medio diario que un trabajador español necesita para eliminar el spam de su buzón de correo oscila entre dos y cuatro minutos. Esto representa una media del 0,63% de la jornada laboral. Aunque no se encuentran publicados los costes y posibles pérdidas económicas se pueden realizar las siguientes estimaciones: si se tiene en cuenta que el coste laboral por empleado en términos netos fue de 26.360 euros en el año 2006[51], el resultado es que las **pérdidas por** productividad de los empleados en las empresas como **consecuencia del spam** se puede situar en **165€ al año por trabajador** que utiliza habitualmente el correo electrónico en su puesto de trabajo**.** Si se considera esta cifra para el año 2007, **las pérdidas representan 179€ al año por trabajador**[52].

Por otra parte, diversos estudios[53] plantean un incremento significativo del volumen de spam, con valores superiores al 70% del total de correos que circulan por la Red a finales del año 2007 y con cifras cercanas al 80%36, en los primeros meses de 2008. Además, el incremento del tamaño de los propios mensajes spam, con las nuevas variantes en ficheros .pdf[54] o .mp3[55], genera la necesidad de prestar servicios de Internet con anchos de banda cada vez mayores, más costosos, que eviten saturaciones y mejoren la calidad.

Estos crecimientos, de la cantidad de spam en circulación y de su tamaño, requieren también de inversiones en infraestructuras de soporte, como dispositivos de almacenamiento con mayor capacidad y sistemas de almacenamiento de respaldo, así como de inversiones en sistemas informáticos (versiones de sistemas operativos actualizadas y estables, servidores de correo

[50] INTECO(2008)
[51] INE(2007)
[52] Estimación sobre el dato del coste laboral bruto del 4º trimestre del 2007 de la "*Encuesta Trimestral de Coste Laboral"*. INE (datos publicados el 14 de marzo de 2008).
[53] MessageLabs y Symantec Corporation.
[54] Por ejemplo: http://blog.hispasec.com/laboratorio/images/noticias/*spam*-pdf.PNG
[55] Por ejemplo: http://www.gfi.com/news/en/mp3spam.htm

más potentes, etc.). A la vez que se invierte en nuevas infraestructuras, las empresas también tienen que invertir en muchos casos en la contratación de nuevo personal cualificado para el mantenimiento de las mismas y la protección frente al spam, generando todo ello un importante sobrecoste económico en inversiones.

Estas inversiones persiguen lograr la fiabilidad en el servicio de correo electrónico. En estas inversiones están involucradas no sólo las empresas proveedoras de servicios de Internet (ISP), sino todas aquellas organizaciones que manejan el correo e incluso, en muchos casos, los propios usuarios privados. Por supuesto, esta inversión es mayor para los ISP, las cuales finalmente trasladan estos gastos en concepto de servicios añadidos a los usuarios finales, con lo cual se puede decir que por este problema finalmente "pagamos todos" los que usamos el correo electrónico.

Como indica el estudio de INTECO[56], es importante que todos los agentes involucrados participen de manera activa en la reducción del impacto que el spam puede causar. Comparando con el resto de las amenazas de seguridad a los sistemas de información, la probabilidad de recepción de un correo spam es más alta, pues las medidas de salvaguardia no consiguen eliminarlos completamente (falsos negativos), con lo que es necesario que los propios agentes inviertan en modernos y actualizados mecanismos de protección antispam. El inconveniente de la aplicación de estos mecanismos es que produce frecuentemente, efectos negativos en el sistema, como retardo en la recepción del correo por la comprobación de los mismos, la limitación de los destinatarios de envío para un mensaje para que no sea considerado spam, las limitaciones de tamaño del buzón de correo y, especialmente, la aparición de falsos positivos que provocan perjuicios para las organizaciones, pues pueden

[56] INTECO(2008)

dar lugar a eliminación de correos legítimos con contenido posiblemente trascendente para los usuarios o las organizaciones. En este caso, en el mejor de los casos los usuarios y técnicos del sistema invertirán un tiempo considerable en la recuperación de esos correos legítimos (entre una hora y una hora y media para la recuperación de un solo mensaje clasificado erróneamente como spam), eso si no han sido eliminados definitivamente, con lo cual las pérdidas monetarias que puede ocasionar la no recepción de esos correos no pueden ser estimadas con precisión.

Resumiendo el cálculo, se puede decir que el coste total que puede ocasionar el spam para las empresas se calcula a partir de la suma de:

- Pérdidas por productividad de los empleados.

-Coste necesario para lograr la fiabilidad del correo electrónico frente al spam:

-Costes de personal.

-Costes de infraestructuras tecnológicas: costes de licencias de herramientas software antispam, y el coste de equipos informáticos de comunicaciones, soporte y almacenamiento.

En este análisis[57] de impacto económico hay que añadir además que el spam, además del ataque a la seguridad, constituye una fuente de propagación de malware, ataques de phishing, etc., con las pérdidas relacionadas que pueden suponer. Aunque es difícil calcular qué pérdidas son provocadas es importante destacar que el uso del spam constituye una de las vías de ataque y propagación más baratas, y por lo tanto, altamente peligrosa. En igual medida, los correos de tipo spam que intentan lograr fraudes piramidales(estafas o scams), desacreditan empresas (cuando hay una suplantación de marca o identidad o brand spoofing y phising, las empresas pueden perder reputación cuando los

[57] INTECO(2008)

spammers les suplantan y provocan fraudes) , difunden publicidad fraudulenta, etc. generan también pérdidas monetarias para organizaciones y usuarios, aunque es prácticamente imposible calcular su acción sobre la economía.

Resumiendo y quedándonos con lo más importante: el spam tiene un coste muy bajo de generar y propagar, puede reportar grandes ingresos a los spammers y compañías que contratan sus servicios, incluso también se benefician las compañías que desarrollan herramientas antispam, etc. aunque no sean parte responsable del problema. En contraposición se genera un sobrecoste (además de la gran molestia que supone el spam) muy importante tanto para las ISP, para las organizaciones y los usuarios particulares, con lo que por unos pocos que obtienen grandes beneficios, otros muchos tantos tienen sobrecostes y molestias de magnitud considerable en mayor o menor medida provocados por un problema que no se puede obviar, el spam.

3.7-El spam en cifras

Internacionalmente, el spam ha alcanzado en los últimos años proporciones preocupantes. Las fuentes de datos son diversas, pero todas coinciden en el incremento de estos correos en los últimos años. Un reciente estudio presentado por Symantec[58] detallaba que, desde el año 2004, se ha producido un incremento progresivo, según los datos correspondientes al primer semestre de 2006, el porcentaje de spam fue de un 54,0%, culminando dicho año con valores del 59,0%; en los informes mensuales de enero y febrero de 2007, el nivel de spam ascendió desde un 60,0% a un 80,0% aproximadamente.

Las razones del rápido crecimiento del spam se encuentran en los bajos costes de entrada (el 98% de los costes son soportados por los receptores)[59], por la posibilidad de ubicar la emisión de spam en máquinas de terceros (a través de troyanos spammers o virus), por los servidores mal configurados o

[58] http://investor.symantec.com
[59] COIT(2004)

alojados en máquinas de países dónde esta práctica no está penalizada y por la falta de seguridad del protocolo utilizado en el envío y la recepción del correo (POP y SMTP), además de por los grandes beneficios que pueden aportar a los agentes implicados como ya hemos visto.

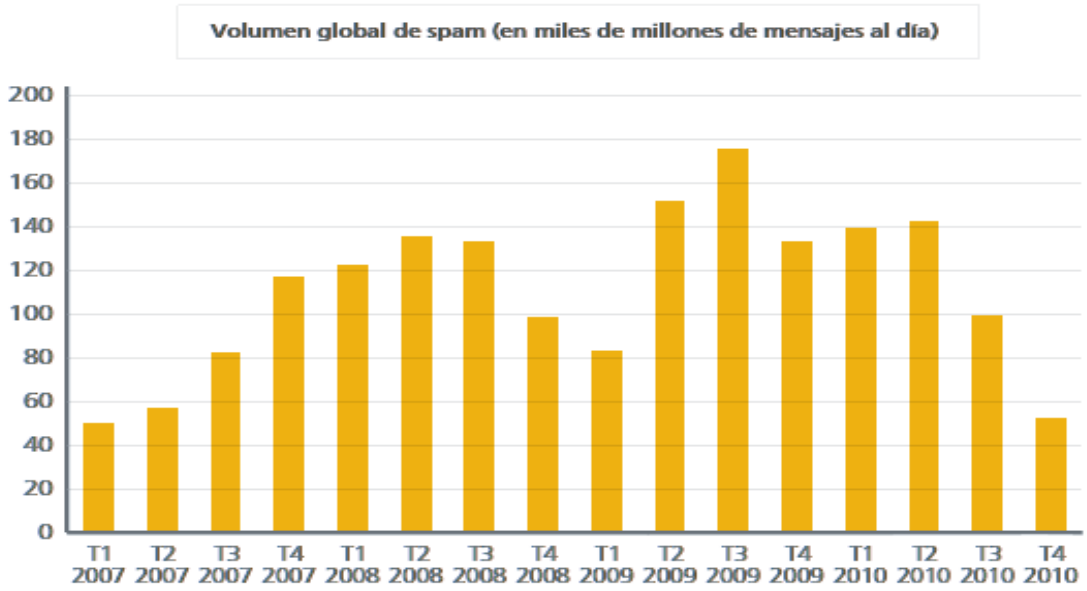
La situación en España es la siguiente: En el 2009 el 88% del correo circulante es spam (casi 9 de cada 10 correos). Sin embargo el número de mensajes que poseen phising y virus ha descendido hasta parámetros de 0,31% y 0,34%, respectivamente[60].

El estudio[61] realizado por INTECO arroja cifras similares: entre el 1 de enero y el 11 de marzo de 2008 el 84,6% de los correos electrónicos que circulaban en España por Internet eran spam.

Atendiendo a los últimos datos disponibles, podemos observar la tendencia de la recepción de spam en los últimos años en el informe[62] elaborado por McAfee sobre amenazas cibernéticas, el cual señala que los volúmenes de spam del último trimestre de 2010 han llegado a su punto más bajo desde el primer trimestre de 2007, hace casi cuatro años. Además, el spam de este último período "sólo" ha supuesto el 80% del total del tráfico de correo electrónico, su prevalencia más baja desde el tercer trimestre de 2006, cuando el tráfico de spam total iniciaba un ascenso meteórico que llegaría a su punto máximo tres años más tarde (2009). Respecto a su punto más alto de la historia, el volumen de spam han caído un 70%, un nivel incluso inferior al que se llegó tras el cierre de **McColo**, un importante proveedor de alojamiento para remitentes de spam, en noviembre de 2008.

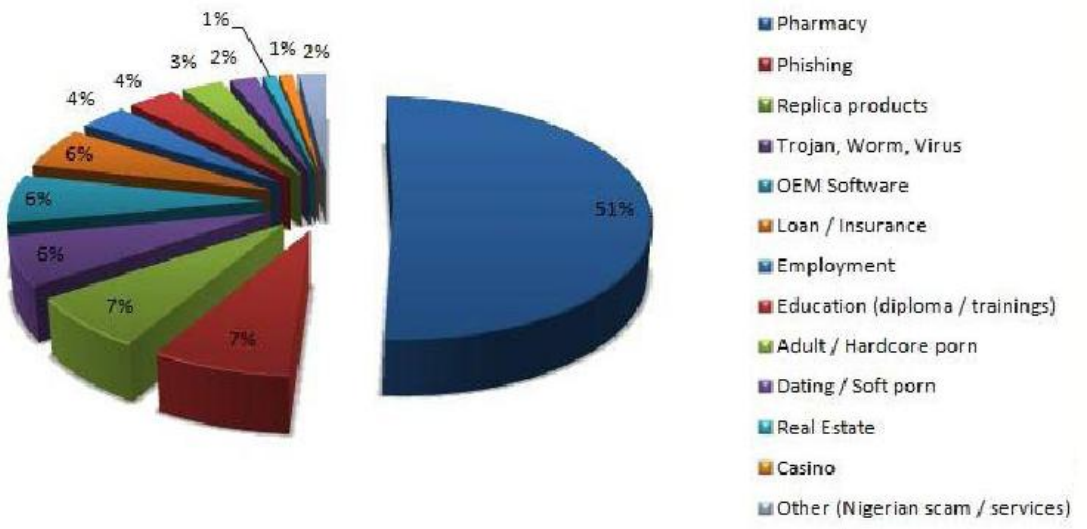
[60] FUNDACION TELEFONICA(2009)
[61] INTECO(2008)
[62] McAfee(2011)

Podemos atender a las cifras de la evolución del spam en los últimos años en la siguiente gráfica que aporta dicho informe de McAfee:



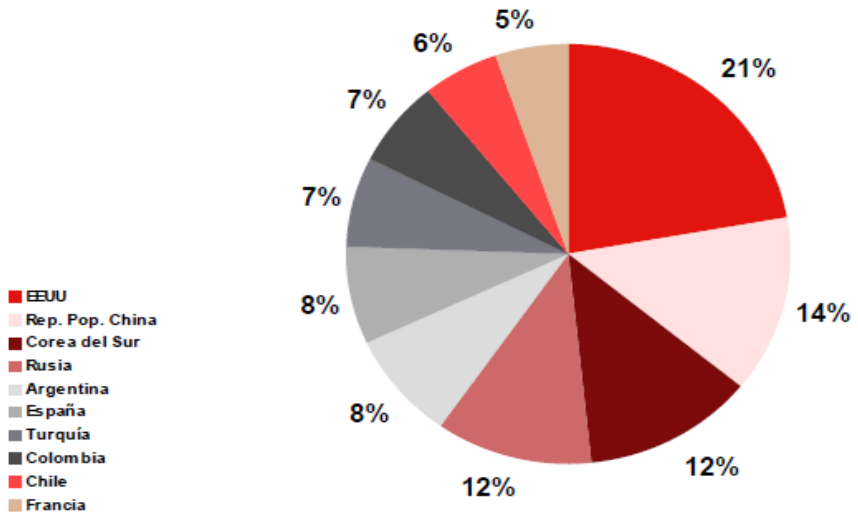
En cuanto a porcentaje de spam recibido según su clase, podemos atender a las proporciones en el "*Informe sobre las amenazas cibernéticas en el segundo semestre de 2009*" de Bit Defender. Los laboratorios de BitDefender antispam estiman que la mayoría de los productos anunciados durante los últimos seis meses de 2009 están relacionados con las ofertas farmacéuticas de Canadá, suponiendo un total del 51 por ciento de todo el spam mundial. Los intentos de phishing enviados por correo electrónico han seguido la misma tendencia que ya se vio en la primera parte del año, aunque las instituciones afectadas han cambiado ligeramente. Podemos apreciar estas cifras en la siguiente gráfica[63]:

[63] BIT DEFENDER(2010)



Atendiendo a los países que son mayores remitentes de spam, en 2008 el volumen analizado por la red de sensores de INTECO indica que entre Estados Unidos, China, Corea del Sur y Rusia envían más del 50% del total de mensajes no deseados o spam que se recibe en España[64]. Podemos observarlo en la siguiente gráfica:

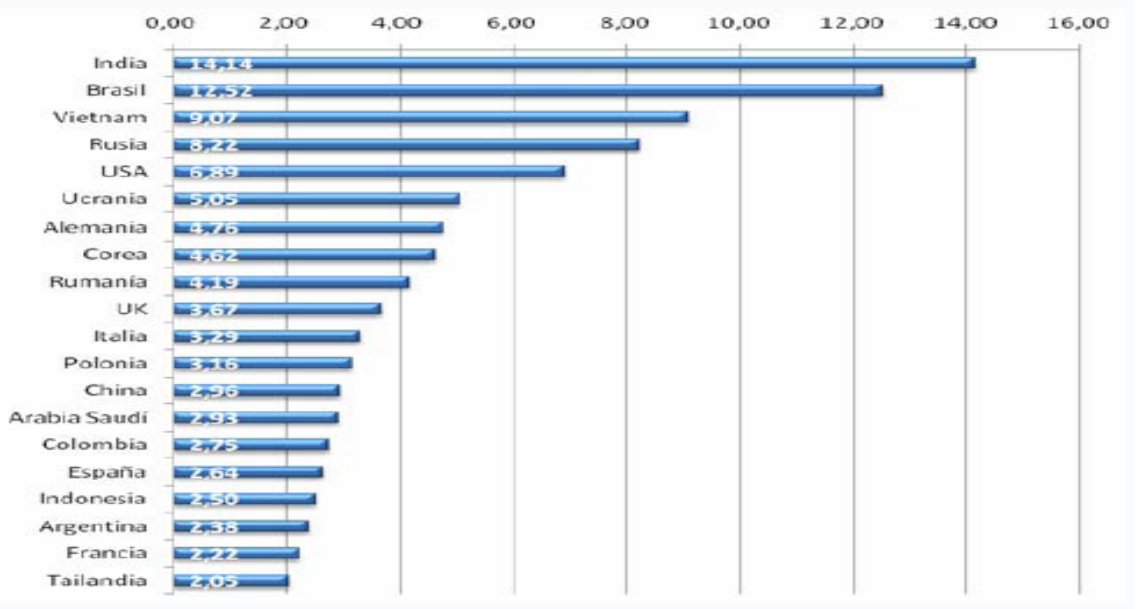
Gráfico 14: 10 países con mayor volumen de *spam* enviado hacia España (%, del 1 de enero al 11 de marzo de 2008)



Fuente: INTECO

[64] INTECO(2008)

Atendiendo a cifras en la actualidad y para ver los mayores generadores de spam a nivel mundial, el informe[65] anual emitido en 2011 y que atiende a las cifras estudiadas en 2010, generado por Panda Security, revela que India, Brasil, Vietnam, Rusia y USA son los mayores generadores de spam a nivel mundial. Podemos ver en la siguiente gráfica los 20 países que son mayores emisores de spam a nivel mundial:



TOP 20 DE PAÍSES EMISORES DE SPAM EN 2010.

En cuanto a la recepción de spam y a las incidencias de seguridad que éste puede acarrear, podemos observar las cifras de evolución recientes en España en la que los usuarios españoles declaran haber sufrido tales incidencias de seguridad, en los últimos períodos. Además, la última columna proporciona los datos reales procedentes de los análisis de INTECO a través de su panel y red de sensores[66]. Apreciamos tales datos en la siguiente tabla[67]:

[65] Panda Security(2011)
[66] Estos datos proceden de la red de sensores de INTECO, disponibles en: https://ersi.inteco.es/index.php?option=com_sanetajax&Itemid=55&lang=es
[67] INTECO(2009)

Tabla 11: Incidencias de seguridad declaradas por los usuarios en función del momento de detección 1T2009 (%)

Incidencia	DECLARADO				REAL
	Nunca	Hace más de un año	En el último año	En los últimos 3 meses	Feb. 09
Virus u otros códigos maliciosos	17,4	31,2	21,0	30,4	63,8
Recepción de correos electrónicos no deseados	6,3	22,2	8,7	62,7	87,4
Víctima de suplantación de identidad	82,5	8,3	4,0	5,2	
Víctima de utilización indebida de datos personales	77,9	13,2	4,4	4,5	
Robo de ancho de banda en la conexión a Internet (intrusión Wi-Fi)	80,3	11,4	4,2	4,1	

Fuente: INTECO

Los problemas que con mayor frecuencia se han producido son los relativos a la recepción de correo electrónico no deseado o spam (la mayor incidencia de seguridad para los españoles) y malware. En la mayoría de los usuarios El 82,5% nunca ha sido objeto de suplantación de identidad, el 80,3% de los usuarios de Internet nunca ha sido víctima de robo de ancho de banda en la conexión a Internet y el 77,9% no ha visto utilizados indebidamente sus datos personales, teniendo un menor peso este tipo de incidencias.

Hay una percepción de los usuarios equivocada, en los últimos tres meses un 62'7% de los hogares declara haber recibido correo no solicitado/deseado, que asciende a 71,4% en el último año. Sólo un 6,3% de los panelistas responden no haber recibido spam en ninguna ocasión. El dato real del spam en febrero de 2009, según la red de sensores de INTECO, supera la percepción de los ciudadanos: del total de correos procesados en febrero de 2009 (392.899.416), un 87,4% se considera spam.

Al spam le sigue, en nivel de incidencia declarada, la existencia de virus u otros códigos maliciosos. Un 30,4% de los usuarios afirma haber sido víctima de malware alguna vez en los últimos 3 meses. Contrastado este dato con el dato real obtenido mediante la herramienta iScan (un 63,8% de equipos infectados por algún tipo de código malicioso en febrero de 2009), la conclusión es clara: existe una importante proporción de ciudadanos que no es consciente de que

sus equipos estén alojando malware. Ello es debido a que la mayor parte del malware detectado (troyanos, spyware) se crea con el objetivo de pasar inadvertido para el usuario y mantenerse oculto en los sistemas infectados (amenazas silenciosas). Al no producir un funcionamiento anómalo del equipo, el usuario no percibe dicha infección por código malicioso en su ordenador.

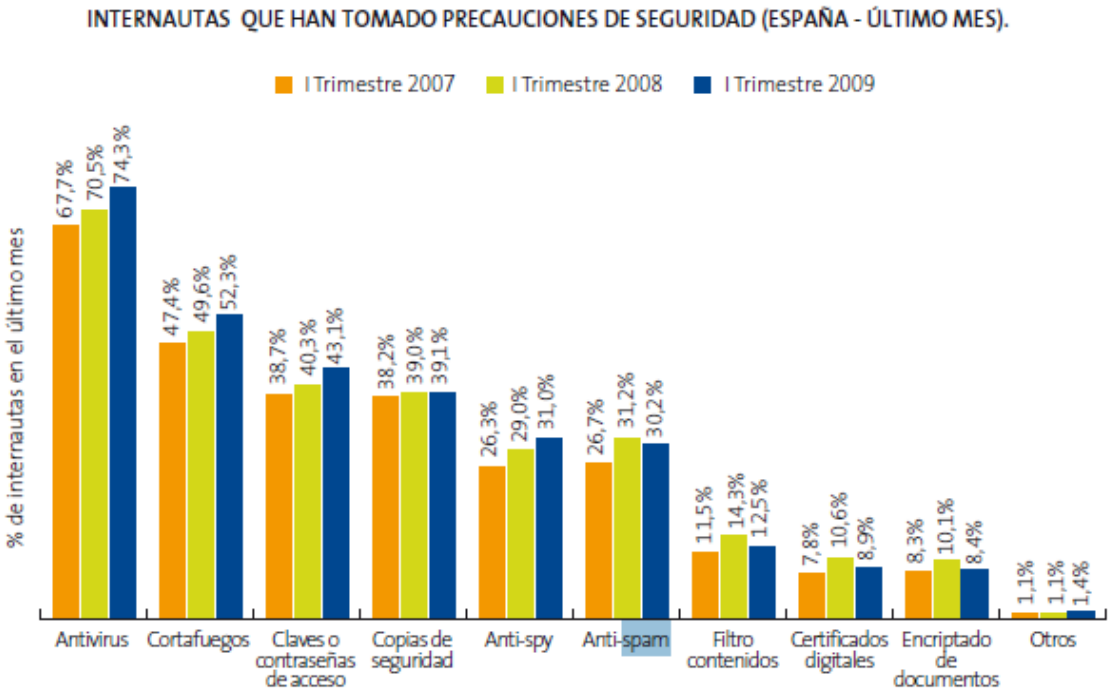
3.8- Medidas en contra del spam

Debido al impacto tanto económico como social que representa el spam en todas sus variantes, de mayor o menor peligrosidad, y debido a que es una de las mayores incidencias de seguridad que sufren los usuarios, se viene experimentando a lo largo del tiempo cada vez una mayor concienciación de este problema, sobre todo cuando el spam pueda provocar una llegada a nuestro ordenador de virus y troyanos que pueden ser capaces de poder "manipular" nuestro PC sin ser conscientes de ello o cuando puede darse un ataque de pishing, o genéricamente poder sufrir cualquier estafa que se inicie en forma de spam. Con lo cual, además de por supuesto en las organizaciones, en España prácticamente la totalidad de usuarios privados toma conciencia del posible problema e intenta adelantarse a él instalando medidas de seguridad en sus computadores, y es que la seguridad sigue siendo un aspecto clave en la expansión de nuevos servicios de la Sociedad de la Información.

Podemos constatar este hecho en el informe[68] de la Fundación Telefónica "*La sociedad de la información en España 2009*", que muestra que en la actualidad los virus (59,6%) y el spam (46,2%) son los dos problemas de seguridad que más afectan a los internautas. Éstos optan como método de protección por herramientas pasivas como los antivirus (74,3%) y cortafuegos (52,3%), en vez de medidas que impliquen cambios en los hábitos como contraseñas (43,1%) o copias de seguridad (39,5%). Podemos ver la evolución

[68] FUNDACION TELEFONICA(2009)

de las medidas de seguridad que toman los usuarios españoles en los últimos años en la siguiente gráfica[69]:



Siguiendo los datos del último "*Estudio sobre la Seguridad de la Información y eConfianza en los hogares españoles*"[70] elaborado por el Observatorio de la Seguridad de la Información de INTECO, y como se muestra en la siguiente tabla, según declaran los usuarios españoles en el 2009, más del 90% de los equipos dispone de programa antivirus, y cerca del 80% utiliza cortafuegos y actualizaciones del sistema operativo. La eliminación de archivos temporales y/o cookies y la utilización de contraseñas, son llevadas a cabo en un 78,3% y 78,1% de los hogares respectivamente, siendo asimismo utilizadas de forma muy considerable. Soluciones más específicas como programas de bloqueo de ventanas emergentes, anti-spam o anti-espía están presentes asimismo en niveles considerables. Podemos apreciar estos datos en la siguiente tabla que realiza comparación con datos del año anterior para ver su evolución:

[69] Fuente: Red.es. "Las TIC en los hogares españoles XXIII oleada".
[70] INTECO(2009)

Medidas de seguridad	1T 08	1T 09	Evolución (puntos porcentuales)
Programas antivirus	89,7	91,2	+1,5
Cortafuegos o *firewall*	71,5	79,2	+7,7
Actualizaciones del sistema operativo y programas instalados	49,4	78,4	+29,0
Eliminación archivos temporales y/o *cookies*	55,7	78,3	+22,6
Contraseñas (equipos y documentos)	49,3	78,1	+28,8
Programas de bloqueo de ventanas emergentes	65,4	74,7	+9,3
Programas anti-spam (correo no deseado)	51,9	65,8	+13,9
Programas anti-espías	51,6	64,8	+13,2
Copia de los discos de restauración del sistema	n.d.	59,8	-
Copias de seguridad de archivos importantes (*backup*)	31,4	59,4	+28,0
Búsqueda de información sobre seguridad informática: artículos, manuales, etc.	n.d.	50,4	-
Partición disco duro	29,2	48,5	+19,3
Programas de filtro de contenidos (control parental para menores)[5]	n.d.	37,1	-
Uso habitual como usuario sin permisos de administrador (con permisos reducidos)	n.d.	35,2	-
Programas anti-fraude	n.d.	32,9	-
Certificados digitales de firma electrónica (FNMT/CERES, etc.)	n.d.	22,5	-
DNI electrónico	n.d.	21,7	-
Cifrado de documentos o datos	9,4	19,2	+9,8

Fuente: INTECO

La evolución en el incremento del uso de las medidas de seguridad es positiva, es posible que esta situación sea en parte la respuesta ciudadana ante las acciones de sensibilización en hábitos seguros de Internet que se están emprendiendo por parte del gobierno, organizaciones, etc.

Además del análisis de las medidas de seguridad que el usuario declara tener instaladas, a continuación podemos ver los datos reales derivados de la auditoría remota de sus equipos[71]. La siguiente tabla contrasta el dato basado en las declaraciones con el resultado real obtenido a través de iScan[72] en febrero de 2009:

[71] INTECO(2009)

[72] Herramienta desarrollada por INTECO que analiza la situación de seguridad de los equipos panelizados.

Tabla 2: Nivel de utilización de medidas de seguridad: datos declarados vs. datos reales 1T2009 (%)

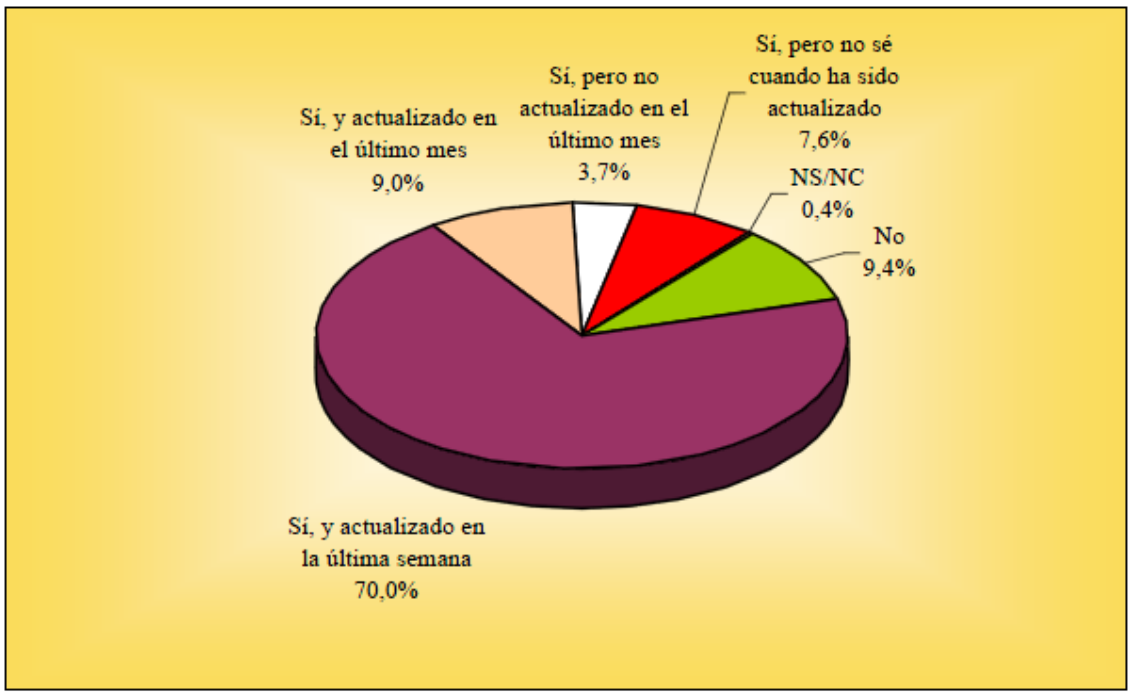
Medidas de seguridad	Declarado	Real	Diferencia (ptos porcentuales)
Programas antivirus	91,2	88,1	± 3,1
Actualizaciones del sistema operativo y programas instalados	78,4	68,1	± 10,3
Uso habitual como usuario sin permisos de administrador (con permisos reducidos)[7]	34,9	17,7	± 17,2

Fuente: INTECO

El nivel real de instalación de cada una de las medidas analizadas es inferior al declarado por los encuestados. En el caso de antivirus, un 88,1% de los equipos realmente lo tienen instalado, frente al declarado por los usuarios (91,2%). El 68,1% de los equipos se detectan como actualizados, frente al 78,4% declarado. Finalmente, el 31,9% de los equipos analizados mantiene vulnerabilidades críticas en el sistema operativo.

Atendiendo a los últimos datos disponibles, referentes al año 2010 en la utilización y actualización de antivirus por parte de los internautas (el antivirus es la medida de seguridad más usada por los usuarios), podemos consultar los datos que nos presenta la Asociación para la Investigación de Medios de Comunicación (AIMC) en su encuesta a usuarios de internet "*Navegantes en la Red*". Podemos apreciar los datos en la siguiente gráfica[73] que atiende a la pregunta formulada a los usuarios internautas: "*¿Tiene instalado algún programa antivirus?*"

[73] AIMC(2010)



Corroborando los datos de la última tabla presentada en la página anterior del estudio de INTECO sobre la materia, la gran mayoría de los españoles usamos como primera medida de seguridad la utilización de antivirus, que además es actualizado frecuentemente por la mayor parte de los usuarios encuestados.

Es importante señalar que además de las medidas de seguridad que puedan tomar los usuarios y de los mecanismos existentes para reducir el spam y los graves problemas que éste pueda ocasionar, los expertos en la materia recomiendan como medida de gran interés y relevancia para la lucha contra el fraude en internet la obligatoria implantación de medidas de seguridad en el software por parte de los fabricantes y proveedores.

En cuanto al posicionamiento y papel actual de los agentes implicados ante el fenómeno del spam, existe un punto en común, la concienciación existente en todas las organizaciones frente al problema del spam.

Los organismos públicos suelen gestionar el correo de manera interna; tanto los equipos como los registros y bases de datos se encuentran en la sede de la

organización, siendo habitualmente el personal encargado de dicha gestión los técnicos pertenecientes a la propia Administración.

La mayoría de las organizaciones de mediano y gran tamaño suelen gestionar de manera interna tanto su sistema de información como su servicio de correo electrónico.

En cuanto a la aplicación de mecanismos antispam, hay que resaltar los siguientes puntos pertenecientes al estudio[74] elaborado por INTECO:

-Las organizaciones actualmente disponen en todos los casos de medidas de seguridad para la protección frente al spam, desde medidas de índole técnico, las más utilizadas, hasta medidas a nivel de la organización y de carácter normativo.

-Las medidas de protección más utilizadas son las reactivas (una vez que éste se encuentra almacenado en el buzón del usuario), como la aplicación de filtros en el análisis del contenido de los correos electrónicos. Estas medidas no pretenden prevenir la recepción de spam, sino el poder tratarlo una vez ha llegado a la bandeja de entrada del e-mail.

-El volumen de spam ha alcanzado tal dimensionalidad que se ha hecho indispensable combatir el problema con anterioridad al almacenamiento del spam en los buzones de los usuarios, siendo necesario el uso de medidas proactivas además de las reactivas comentadas en el anterior punto.

-Es habitual la utilización de mecanismos de protección basados en listas de filtrado de direcciones (**blancas**: direcciones de correo-e permitidas que no son generadoras de spam y permiten la recepción del e-mail, **negras**: listas de correo que envían spam y bloquean el e-mail antes de llegar a la bandeja de entrada, o **grises**: el resto de direcciones en las que no hay certeza todavía de a qué clase pertenecen).

-Asimismo existe el uso de **filtros bayesianos** o adaptativos que no clasifican los mensajes por la dirección IP de procedencia, sino que lo hacen mediante

[74] INTECO(2008)

las palabras que contiene el mensaje y su frecuencia. Al recibirse un mensaje, el filtro compara su contenido con una lista de palabras no aceptadas, analiza el contexto y calcula la probabilidad de que sea spam. Estos filtros evolucionan paralelamente al spam, de modo que si cambian las palabras los filtros lo reconocen automáticamente. No evitan uno de los problemas básicos del spam, que es que los servidores de correo se colapsen.

-Una aspecto interesante en cuanto a los servicios antispam empleados por los agentes estudiados es la tendencia a redirigir el correo a otras entidades para su filtrado.

Asimismo, además hay una serie de pautas recomendables para prevenir o reducir el volumen de recepción de SPAM que pueden realizar los usuarios. Y así y con motivo de la primera celebración del día de Internet, el 25 de octubre de 2005, la Agencia Española de Protección de Datos elabora un decálogo con recomendaciones para combatir el spam[75], en la que se recogen las principales medidas para prevenir y combatir este fenómeno:

1- Ser cuidadoso al facilitar la dirección de correo.

2- Utilizar dos o más direcciones de correo electrónico.

3- Elegir una dirección de correo poco identificable por el spammer.

4- No publicar la dirección de correo (en buscadores, directorios de contactos, foros o páginas Web). Si es necesario publicarla sustituir "@" por "arroba". Para mandar un correo a múltiples direcciones, enviarlo con copia oculta. Si reenvía un correo, elimine las direcciones de los anteriores destinatarios.

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

[75] Disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/index-ides-idphp.php

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

7- No es conveniente contestar al Spam.

8- No pinche sobre los anuncios de los correos basura (en ningún enlace).

9- Utilice filtros de correo antispam.

10- Mantenga al día su sistema. Utilice programas antivirus, cortafuegos, actualizaciones y parches.

Hay que resaltar que la AEPD (Agencia Española de Protección de Datos) es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos en España. La **entrada en vigor de normas en materia de Telecomunicaciones y Servicios de la Sociedad de la Información** atribuye a la Agencia la tutela de los derechos y garantías de abonados y usuarios en el ámbito de las comunicaciones electrónicas. Entre ellas, la **defensa de la privacidad de los usuarios de Internet frente al Spam.**

4- Aspectos legales del spam

Este apartado del proyecto ha sido elaborado a partir del estudio de INTECO "Estudio sobre la situación, naturaleza e impacto económico y social del correo electrónico no deseado 'spam'", añadiendo información citada encontrada en otros medios y comentarios propios.

El correo electrónico no deseado (spam) en forma de comunicaciones comerciales a través de este medio (correo electrónico) es un instrumento de promoción empresarial y una actividad publicitaria en sí misma, que se ha convertido en una de los métodos de marketing más utilizados por las empresas. Pero el ejercicio abusivo y agresivo de dichas técnicas ha supuesto la reacción del legislador, promulgando una normativa específica para proteger a los consumidores y usuarios. Junto con la regulación de su contenido, dirigida a hacer de ellas actividades veraces y transparentes, se procura que las comunicaciones comerciales enviadas a través de Internet sean totalmente identificables como tales y que se haga un uso lícito de los datos personales utilizados para preparar las promociones a través del correo electrónico.

Las comunicaciones comerciales enviadas a través de la Red ofrecen innumerables ventajas, pero también ciertas incertidumbres jurídicas que precisan del establecimiento de un marco jurídico adecuado. Diariamente estas prácticas de difusión comercial masiva son poco respetuosas con el derecho a la intimidad y a la privacidad de las personas; en particular, las intromisiones no deseadas y la difusión de datos personales con finalidad comercial, fuente de gran parte de las ofertas y de la publicidad no deseada.

Estas prácticas suelen ir acompañadas con relativa frecuencia de una violación de la normativa vigente en materia de protección de datos, ya que para formar una base con direcciones de e-mail no cuentan con el consentimiento de los titulares de dichos datos.

En cualquier caso, es necesario recordar que este tipo de publicidad no puede suponer en modo alguno un menoscabo de los derechos y legítimos intereses de sus destinatarios, al igual que ocurre con el resto de formas de publicidad que se realizan a través de otros medios.

Por todo ello, en los sucesivos apartados del presente proyecto, se recopilará el régimen jurídico de las comunicaciones comerciales vía electrónica en su conjunto, desde su definición y normativa aplicable, pasando por los requisitos que los empresarios deben cumplir para enviar comunicaciones que no hayan sido solicitadas por los destinatarios de las mismas, hasta el sistema de responsabilidad correspondiente a las infracciones cometidas y daños ocasionados en la materia, y desde un punto de vista amplio, ya que no se estudiará sólo la legislación española sino el origen de la misma, que se encuentra en el ámbito de la Comunidad Europea (la protección de los consumidores es uno de los principios básicos de la Unión Europea, recogido como política autónoma en el artículo 153 del Tratado de la Comunidad Europea).

Existen pocas referencias especializadas en la materia, a pesar de tener gran importancia para la reducción de los efectos de las comunicaciones electrónicas no deseadas y del fenómeno spam. Se detallan a continuación la terminología y definiciones empleadas por la normativa, la garantía de los derechos y obligaciones de los destinatarios y entidades emisoras de correo masivo, la protección de datos personales involucrada, así como el régimen sancionador aplicable.

4.1- Consideraciones previas sobre el correo electrónico no deseado (spam)

Se puede afirmar que el spam es una adaptación a la nueva Sociedad de la Información de la tradicional propaganda enviada por correo postal, debido a las similares molestias que ambos presentan.

En cuanto al concepto de spam, actualmente no existe ni en la doctrina ni en el Derecho comparado unanimidad a la hora de determinarlo, entendiéndose genéricamente como todo aquel e-mail no solicitado que llega a los buzones de correo electrónico, independientemente del tema tratado. También se define el spam como aquellos correos electrónicos comerciales no solicitados y masivos no solicitados procedentes de una misma persona. Lo que resulta común en ambas definiciones es que se trata de correos electrónicos no solicitados, pero dicha condición, aun siendo necesaria, no es requisito suficiente para considerarlo como tal, pues el rasgo que lo cualifica es su carácter comercial o la cantidad enviada (si es masiva o no).

En el ordenamiento jurídico español los correos electrónicos no deseados de contenido no comercial no han tenido un tratamiento legal, ya que la legislación española se ha centrado única y exclusivamente en la regulación del que se podría denominar spam comercial, correos electrónicos comerciales no deseados o comunicaciones comerciales no solicitadas. La legislación española emplea el término de comunicaciones comerciales no solicitadas para referirse a este tema, que es donde se centrará en el estudio legal del presente proyecto.

Es importante no confundir el término genérico de spam con la prospección comercial no solicitada de las empresas, que no siempre es spam, ya que está permitido enviar comunicaciones comerciales no solicitadas cuando se cumple la normativa vigente, como se verá más adelante.

4.2- Marco jurídico aplicable al fenómeno del spam en España

-Definición de las comunicaciones comerciales vía electrónica

Las comunicaciones comerciales se pueden entender como todo aquel mensaje publicitario destinado a impulsar una actividad comercial a través de cualquier medio de comunicación. Su definición legal se recogió, por primera vez, en la Directiva comunitaria 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de

los servicios de la Sociedad de la Información, en particular del comercio electrónico en el mercado, más conocida como Directiva sobre Comercio Electrónico (en adelante DCE).

En dicho apartado se pueden diferenciar dos partes. Por un lado, señala que se entiende por comunicación comercial *"todas las formas de comunicación destinada a proporcionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o profesiones reguladas"*. Por otro lado, completa la citada definición con aquellas actividades que no se consideran como tales; en concreto*, "no se consideran comunicaciones comerciales ni los datos que permitan acceder directamente a la actividad de la empresa, organización o persona y, en particular, el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, servicios o a la imagen de la empresa, organización o persona elaboradas de forma independiente a ella, en particular cuando se realicen sin contrapartida económica"*[76].

En el ordenamiento jurídico español, la Ley 34/2002 de Servicios de la Sociedad de la Información y Comercio Electrónico, de 11 de julio, denominada Ley de Comercio Electrónico o en adelante LSSICE, que traspone la mencionada Directiva (2000/31/CE), recoge el concepto de comunicación comercial de forma muy similar que la susodicha Directiva, definiendo las comunicaciones comerciales como *"toda forma de comunicación dirigida a la promoción directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional"*, excluyendo de tal definición *"los datos que permiten acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones*

[76]Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información, en particular del comercio electrónico en el mercado. Artículo 2. Párrafo f)

relativas a los bienes, los servicios o la imagen que se ofrezcan cuando sean elaboradas por un tercero y sin contraprestación económica"[77].

Por tanto, se excluyen del concepto de comunicaciones comerciales las actividades desarrolladas por terceros sin encargo del titular de los bienes o servicios y sin remuneración, los enlaces a páginas web de contenido publicitario o la indicación de direcciones de correo electrónico.

Aunque no se mencionan explícitamente, quedarían asimismo excluidas del concepto de comunicaciones comerciales todas aquellas que tienen meramente carácter informativo, ausentes de toda finalidad comercial o empresarial como la propaganda institucional, política y religiosa.

En consecuencia, tanto la Directiva como la LSSICE, al hacer referencia a la expresión "toda forma de comunicación", abarcan un concepto muy amplio de comunicación comercial en el que se incluyen todas las comunicaciones comerciales emitidas online, salvo las excepciones puntualizadas, independientemente de la forma y el formato que los mensajes reciban (gráfico, audio, audiovisual).

-Normativa aplicable a las comunicaciones comerciales vía electrónica

Las comunicaciones comerciales vía electrónica no sólo se regirán por la LSSICE, sino que se aplicarán otras normas, tal y como lo establece el artículo 19 (Régimen jurídico) de la LSSICE, que especifica las leyes aplicables a las mismas: "*además de por la presente Ley, por su normativa propia y la vigente en materia comercial y de publicidad"*.

Por tanto, cuando se envíen comunicaciones comerciales será de aplicación: la Ley 34/1988, de 11 de noviembre, General de Publicidad (en adelante, LGP), que delimitará la ilicitud de las actividades publicitarias; el artículo 20 LSSICE y, supletoriamente, el Título II de la Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista (en adelante LOCM) en lo referente a la modalidad y

[77] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Anexo. Párrafo f)

contenido de las comunicaciones como actividad de promoción o marketing; la Ley 26/1984, de 19 de julio, General de Defensa de los Consumidores y Usuarios (en adelante, LGDCU), y la Ley Orgánica de Protección de Datos (en adelante, LOPD) en lo que concierne al tratamiento de datos personales.

-LAS COMUNICACIONES COMERCIALES NO SOLICITADAS

Actualmente el mayor problema del envío de comunicaciones comerciales vía electrónica es la recepción de correos electrónicos no solicitados o spam. Por tanto, al suponer un problema para sus destinatarios, la legislación española ha establecido unos requisitos, que se detallan a continuación, para poder enviar comunicaciones comerciales no solicitadas válidamente.

-Sujetos protegidos frente al envío de comunicaciones comerciales no solicitadas

El envío de comunicaciones comerciales es un servicio de la Sociedad de la Información cuyos destinatarios son personas físicas o jurídicas. La LSSICE ampara tanto a las personas físicas como a las personas jurídicas destinatarias del servicio frente al envío de comunicaciones comerciales no solicitadas.

-La regulación en el derecho español en el envío de comunicaciones comerciales no solicitadas

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, establece que "***Sólo se podrá autorizar la utilización de*** *sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o* ***correo electrónico con fines de venta directa respecto de aquellos abonados que***

hayan dado su consentimiento previo.”[78]. Aquí se ha considerado la modalidad más beneficiosa para el destinatario estableciendo el sistema conocido como **opt-in**.

Hay que destacar que es importante la elección de esta modalidad por la legislación europea, y consecuentemente por la española, ya que supone desmarcarse del sistema americano que prohíbe el envío de mensajes por correo electrónico cuando el destinatario haya manifestado previamente su oposición a ello, es decir, el denominado sistema **opt-out.**

Semejante a la anterior directiva europea mencionada, la LSSICE establece que “*queda* ***prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente*** *que previamente* ***no*** *hubieran sido* ***solicitadas o*** *expresamente* ***autorizadas*** *por los destinatarios de las mismas*”[79].

El correo electrónico se presenta como uno de los medios de comunicación señalados por dicha ley para remitir comunicaciones comerciales no solicitadas, pero el ordenamiento jurídico español no contiene ninguna definición de correo electrónico, puesto que la LSSICE no la recogió dentro de su amplio anexo de definiciones. Por tanto, se debe acudir a la Directiva 2002/58/CE europea, donde el correo electrónico se define como *“todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo”*[80].

Retornando a la última norma mencionada de la LSSICE, la que incluye la expresión *“**comunicación electrónica equivalente**”*, se puede concluir según apunta la última directiva europea mencionada, que se entiende por ésta el

[78]Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Artículo 13, párrafo 1,

[79] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 21.

[80] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Artículo 2 h)

envío de mensajes mediante telefonía móvil, y se excluyen los servicios de telefonía vocal, fax o télex.

-El consentimiento en el envío de comunicaciones comerciales no solicitadas

Como se había comentado anteriormente, el artículo 21 de la LSSICE establece la prohibición de enviar comunicaciones comerciales publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente **no** hubieran sido **solicitadas o expresamente autorizadas** por los destinatarios de las mismas. Por tanto, la ley española obliga a las empresas a que las comunicaciones electrónicas hayan sido previamente solicitadas por los destinatarios de las mismas o a solicitar el consentimiento expreso de los destinatarios de los mensajes.

En consecuencia, si se da la primera condición de que las comunicaciones hayan sido solicitadas no hay ningún problema, pero en la segunda condición de consentimiento expreso de los destinatarios se pueden plantear problemas que se detallan seguidamente:

El consentimiento expreso

En la obtención del consentimiento expreso de los destinatarios por parte de las empresas es donde se encuentran los principales problemas para el envío de comunicaciones comerciales, ya que en la práctica las empresas no suelen solicitar el consentimiento expreso, sino que ofrecen únicamente la posibilidad de darse de baja del servicio enviando un mensaje de correo electrónico o accediendo a determinados enlaces. Esto no supone dar la autorización expresa para recibir comunicaciones comerciales no solicitadas, sino un consentimiento tácito.

Para obtener el consentimiento de los destinatarios de las comunicaciones comerciales, las empresas utilizan distintos métodos, normalmente los siguientes:

-Las casillas marcadas previamente.

-Las casillas seleccionables.

-La doble manifestación del destinatario de las comunicaciones comerciales confirmando su inscripción mediante el envío de un mensaje automático a su buzón.

En conclusión, la exigencia del consentimiento expreso que establece la LSSICE aumenta considerablemente las restricciones para el emisor de la comunicación comercial y las garantías para el destinatario, además de aumentar la exigencia respecto de la LOPD, que únicamente exige un consentimiento inequívoco, puesto que la LSSICE no permite admitir el consentimiento tácito e implícito en el envío de comunicaciones comerciales no solicitadas. Con lo cual en la práctica, las empresas remitentes de comunicaciones comerciales no solicitadas ya no pueden enviar correos electrónicos que ofrezcan al destinatario la posibilidad de no recibir más promociones no solicitadas, como ocurría hasta la entrada en vigor de la LSSICE.

El consentimiento incluido dentro de un proceso contractual

Normalmente los destinatarios de las comunicaciones comerciales son los clientes de las empresas remitentes, y en este supuesto se excluye el requisito del consentimiento expreso, tal y como establece el párrafo segundo del artículo 21 LSSICE, que afirma que "*no será de aplicación el requisito del consentimiento expreso cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente*".

Es decir, para eximirse la empresa del requisito de la obtención del consentimiento expreso del destinatario cuando envía comunicaciones

comerciales no solicitadas, es necesario que haya existido entre éste y dicho destinatario una "relación contractual previa", es decir, tuvo que haber existido o una venta concluida o negociaciones previas con tal destinatario para cualquier contrato y en cualquier momento, ya que la ley no especifica nada más. Con lo cual, por el simple hecho de haber comprado en un determinado comercio tiempo atrás, una persona puede recibir sin previo aviso correos electrónicos no solicitados sobre otros productos de la firma.

Además, dicho artículo señala que, "*en todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de la recogida de los datos como en cada una de las comunicaciones comerciales que le dirija"*. Con lo cual, en el contexto español, el destinatario de las comunicaciones comerciales no solicitadas en cualquier momento puede darse de baja del servicio de recepción de dichas comunicaciones con una revocación del consentimiento o autorización como se puede ver en los puntos que se desarrollan a continuación.

-Otros requisitos legales de las comunicaciones comerciales: Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos

Las comunicaciones comerciales electrónicas que se realicen por correo electrónico u otro medio de comunicación electrónica, además de haber sido expresamente autorizadas como ya se ha visto, deben reunir los siguientes tres requisitos que recoge el artículo 20 de la LSSICE:

1- *"Las comunicaciones comerciales deberán ser claramente identificables como tales"* [81]

[81] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 20. Párrafo 1.

A tal respecto, el artículo 6 de la DCE no incluye ninguna palabra o frase modelo común para todos los estados miembros y que haga más uniforme la identificación por los receptores de las comunicaciones comerciales, sino que exige, de forma general, que las comunicaciones comerciales como mínimo sean claramente identificables como tales, a diferencia de la legislación estadounidense, en la cual se utiliza la expresión "*spam*" como fórmula más utilizada para especificar el contenido del mensaje.

En cambio, en la legislación española, a diferencia de la europea, sí se entra en este aspecto. Se apunta después de señalar el citado requisito, que "*en el supuesto en el que las comunicaciones comerciales se realicen a través de correo electrónico o medios electrónicos equivalentes se deberá incluir al comienzo del mensaje la palabra "publicidad"' "*, o la abreviatura "publi" si se modifica el citado artículo 20 LSSICE a través de la promulgación del actual Proyecto de Ley de Medidas de Impulso de la Sociedad de la Información.

Con lo cual, cuando se envíen correos electrónicos comerciales no deseados se deberá identificar el mismo con la palabra "publicidad" al comienzo del mensaje, pero dicha ley no señala exactamente qué debe entenderse con la expresión "al comienzo", sino que lo contempla como un lugar general, a diferencia de multitud de estados norteamericanos que exigen que conste una palabra o unas siglas al principio del encabezamiento del mensaje.

2- *"Las comunicaciones comerciales deberán indicar la persona física o jurídica en nombre de la cual se realizan los envíos"*[82]

La intención aquí es que el destinatario de las comunicaciones comerciales conozca el origen o procedencia de la misma. Hay que destacar que se señala como persona a incluir en la comunicación comercial no solicitada la persona **en nombre de quien** se realiza el envío, que no tiene por qué coincidir con quien envía el mensaje. De hecho en el ámbito de la publicidad, casi siempre no

[82] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 20. Párrafo 1.

coincidirá, ya que la empresa que realiza el envío efectivo de las comunicaciones comerciales es una organización contratada para ello, quedando reflejada en tal comunicación la persona física o jurídica que contrató a tal empresa publicitaria, que es la representante de tal comunicación comercial.

Consecuentemente a dicha consideración legal, las empresas deberán asegurarse de con quién contrata los servicios de distribución de su publicidad, ya que por un mal uso de este servicio se pueden imponer sanciones por incumplimiento de la ley para la empresa anunciante además del deterioro de su imagen.

3- *"En los supuestos de que las comunicaciones comerciales sean ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales se exige que se identifiquen claramente como tales y que las condiciones de acceso o participación se expresen de forma clara e inequívoca"*[83]

Resaltar que por "condiciones de acceso", deberá entenderse la inclusión de la duración de la oferta y, en su caso, las reglas especiales aplicables a la misma. Se busca así garantizar que el anuncio de una promoción contenga un contenido ventajoso al que se pueda acceder con facilidad.

Es importante señalar asimismo que se ha tramitado en la Unión Europea un reglamento relativo a las promociones de ventas en el mercado interior, concretamente la Propuesta COM/2001/0546 modificada por la Propuesta COM/2002/0585. La aprobación de esta propuesta de reglamento ha supuesto modificaciones considerables y, sobre todo, la unificación de esta materia en el Derecho europeo en donde existen notables diferencias.

[83] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 20. Párrafo 2.

-Revocación del consentimiento

Recordar que además de deber cumplir los requisitos anteriores para enviar comunicaciones comerciales no solicitadas, las empresas deben ofrecer la posibilidad al destinatario de las comunicaciones, que consintió en su día el envío de comunicaciones publicitarias, de revocar la autorización en cualquier momento con simplemente la notificación de tal voluntad al remitente, mediante la habilitación de un procedimiento sencillo y gratuito, como cita el artículo 22 de la LSSICE: *"El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente".* Y añade:

"A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado".

"Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos".[84]

-Infracciones y sanciones en el ámbito de las comunicaciones comerciales no solicitadas

Para asegurar la protección de los usuarios en materia de la recepción de las comunicaciones comerciales no solicitadas hay establecido un régimen disciplinario con el fin de garantizar el cumplimiento de la legislación. Para tal fin, el artículo 37 de la LSSICE establece que los prestadores de servicios de la Sociedad de la Información, cuando les sea de aplicación la citada ley (LSSICE), estarán sujetos al régimen sancionador de la misma.

Se puede consultar el artículo 38 de la LSSICE para catalogar la gravedad de las infracciones, que se calificarán como muy graves, graves y leves. A continuación se entra en detalle en las mismas.

[84] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 22. Párrafo 2.

Son infracciones muy graves:

1- El incumplimiento de las órdenes dictadas en virtud del artículo 8 (Restricciones a la prestación de servicios cuando atentan contra principios básicos) en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.

2- El incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red o la prestación de cualquier otro servicio equivalente de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11 (Deber de colaboración de los prestadores de servicios de intermediación).

3- El incumplimiento de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12.

4- La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.

Las infracciones muy graves prescribirán a los tres años[85], y se impondrán sanciones económicas con multas de 150.001 hasta 600.000 euros[86], que prescribirán a los tres años.

Son infracciones graves:

1- El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a destinatarios que no hayan autorizado o solicitado expresamente su remisión, o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios

[85] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 45.

[86] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 39.1 párrafo a)

aludidos a un mismo destinatario, cuando en dichos envíos cuando éste no hubiera solicitado o autorizado su remisión.

Con lo cual, en este párrafo del artículo se consideran dos supuestos como infracciones graves:

-El envío masivo de comunicaciones comerciales electrónicas.

-El envío de más de tres comunicaciones comerciales en el plazo de un año al mismo destinatario.

En cuanto al segundo supuesto, es muy importante la cantidad de comunicaciones comerciales enviadas, ya que si sólo se puede demostrar el envío de tres comunicaciones comerciales al mismo destinatario, la infracción sería calificada como leve (para ser grave han de ser más de tres envíos) y la multa difiere notoriamente de las infracciones graves, y además éstas pueden conllevar aparte de la sanción económica, el establecimiento de medidas provisionales en contra del remitente de las comunicaciones.

Respecto al primer supuesto, a pesar de que no se recoge su significado, puede deducirse que el concepto de "envío masivo de mensajes" no considera el supuesto de que se envíen muchos mensajes a un solo destinatario, en cuyo caso sería la infracción anterior (el segundo supuesto), sino que hace referencia a los casos en que se envía un solo mensaje a muchos destinatarios.

Existe un inconveniente en esta parte y es que no se determina en dicho artículo si el envío masivo se produce cuando se envían muchos correos electrónicos simultáneamente o cuando se envía de manera habitual comunicaciones comerciales no solicitadas. A continuación se continúa con los supuestos para darse una infracción grave.

2- El incumplimiento significativo de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con la solicitud del consentimiento expreso del destinatario.

3- El incumplimiento significativo de las obligaciones de información por parte del prestador de servicios establecidas en los párrafos a) y f) del artículo 10.1, o el incumplimiento del establecimiento de un procedimiento sencillo y gratuito para la revocación del consentimiento prestado por el destinatario, establecidas en el apartado 2 del artículo 22.

4- No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27, relativos a las obligaciones previas al inicio del procedimiento de contratación.

5- El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación del contrato, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor.

6- La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.

Las infracciones graves prescribirán a los dos años[87] y se impondrán sanciones económicas con multas de 30.001 hasta 150.000 euros[88] que prescribirán a los dos años.

Son infracciones leves:

1- El incumplimiento de lo previsto en el artículo 20 para las comunicaciones comerciales, ofertas promocionales y concursos.

2- El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente a los destinatarios que no hayan solicitado o autorizado expresamente su remisión, cuando no constituya infracción grave.

[87] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 45.

[88] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 39.1 párrafo b)

3- El incumplimiento de las obligaciones de información establecidas en los párrafos a) y f) del artículo 10.1, o del establecimiento de un procedimiento de revocación del consentimiento expreso prestado por el destinatario, establecidas en el apartado 2 del artículo 22, cuando no constituya una infracción grave.

4- El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación la solicitud del consentimiento expreso del destinatario.

5- La falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la sociedad de la información.

6- No facilitar la información a que se refiere el artículo 27.1 (Obligaciones previas al inicio del procedimiento de contratación), cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.

7- El incumplimiento de la obligación de confirmar la recepción de una aceptación del contrato, en los términos establecidos en el artículo 28 (Información posterior a la celebración del contrato), cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.

Las infracciones leves prescribirán a los seis meses[89] y se impondrán sanciones económicas con multas de hasta 30.000 euros[90] que prescribirán al año.

Se puede apreciar que el intervalo de la cuantía en las sanciones es bastante amplio, por ello el artículo 40 LSSICE establece los siguientes criterios para la graduación de la cuantía de la multa:

[89] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 45.

[90] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 39.1 párrafo c)

1- La existencia de intencionalidad.

2- El plazo de tiempo durante el que se haya venido cometiendo la infracción.

3- La reincidencia por comisión de infracciones de la misma naturaleza, cuando así haya sido declarado por resolución firme.

4- La naturaleza y cuantía de los perjuicios causados.

5- Los beneficios obtenidos por la infracción.

6- El volumen de facturación a que afecte la infracción cometida.

Además de las sanciones señaladas, "*las infracciones graves y muy graves podrán llevar aparejada la publicación, a costa del sancionado, de la resolución sancionadora en el Boletín Oficial del Estado, en el diario oficial de la Administración Pública que, en su caso, hubiera impuesto la sanción, en dos periódicos cuyo ámbito de difusión coincida con el de la actuación de la citada Administración o en la página de inicio del sitio de Internet del prestador, una vez que aquella tenga carácter firme*". Además en el citado artículo se señala que "*Para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, el número de usuarios o de contratos afectados, y la gravedad del ilícito*".[91].

El órgano competente para imponer las sanciones señaladas será, de conformidad con el artículo 43 de la LSSICE, el Ministro de Ciencia y Tecnología, que en la actualidad correspondería al Ministro de Industria, Turismo y Comercio, en el caso de infracciones muy graves, y el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información en el supuesto de infracciones graves y leves.

Aun así, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que

[91] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 39. Párrafo 2.

se trate a que se refieren los párrafos a) y b) del artículo 38.2 de esta ley (LSSICE) para las infracciones muy graves, corresponderá al órgano que dictó la resolución incumplida.

Asimismo, corresponderá a la Agencia Española de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) para infracciones graves y 38.4 d), g) y h) en infracciones leves, de esta misma ley.

Además, "*los procedimientos sancionadores por infracciones graves o muy graves se podrán adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y sus normas de desarrollo, las medidas de carácter provisional previstas en dichas normas que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales*", según indica el artículo 41 de la LSSICE. En particular, podrán acordarse las siguientes medidas de carácter provisional:

1- Suspensión temporal de la actividad del prestador de servicios y, en su caso, cierre provisional de sus establecimientos.

2- Precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo.

3- Advertir al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas.

Como siempre, se respetará, en todo caso, el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

En el supuesto que no se cumplan las medidas provisionales, "*el órgano administrativo competente para resolver el procedimiento sancionador podrá*

imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas", según señala el artículo 42 de la LSSICE.

Por último, es muy importante destacar que las obligaciones que garantizan la licitud de las comunicaciones comerciales no solicitadas remitidas por vía electrónica van a ser exigibles tanto a los prestadores de los servicios de la Sociedad de la Información emplazados en España, según indica el artículo 2 de la LSSICE, como a aquellos que se encuentren establecidos en un país miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España, según se desprende del artículo 3 de la citada ley. Además para el resto de casos en este contexto de ilicitud, con una ubicación fuera de la comunidad europea, la LSSCICE señala que "*Cuando las infracciones sancionables con arreglo a lo previsto en esta Ley hubieran sido cometidas por prestadores de servicios establecidos en Estados que no sean miembros de la Unión Europea o del Espacio Económico Europeo, el órgano que hubiera impuesto la correspondiente sanción podrá ordenar a los prestadores de servicios de intermediación que tomen las medidas necesarias para impedir el acceso desde España a los servicios ofrecidos por aquéllos por un período máximo de dos años en el caso de infracciones muy graves, un año en el de infracciones graves y seis meses en el de infracciones leves*"[92].

-Responsabilidad de los intermediarios

El uso ilícito de Internet puede causar daños y perjuicios a terceros que se han de reparar. Y para poder alojar, almacenar o transmitir los contenidos ilícitos en la Red es necesaria la intervención técnica de los prestadores de servicios de intermediación. Pues bien, la cuestión estriba en determinar qué

[92] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 39. Párrafo 3.

responsabilidad tendrán tales prestadores de servicios de intermediación. Se atenderá a ello en los siguientes puntos del presente proyecto.

A tal efecto, en el ámbito comunitario se adoptó el sistema de responsabilidad de los prestadores del servicio en la Directiva sobre Comercio Electrónico (DCE), donde se reconocen una serie de supuestos específicos de exención de responsabilidad que se aplicarán cuando se cumplan los requisitos señalados para cada una de ellas; cuando no se cumplan tales requisitos, será aplicable entonces el sistema general de responsabilidad de la legislación española.

-La exención de responsabilidad civil por contenidos ajenos en Internet

Las exenciones de responsabilidad establecidas tanto en la DCE como en la LSSICE sólo se aplican en aquellos casos en los que la actividad del prestador de servicios de la Sociedad de la Información se limita al proceso técnico de explotar y facilitar el acceso a una red de comunicación mediante la cual la información facilitada por terceros es transmitida o almacenada temporalmente, con el fin de hacer que la transmisión sea más eficiente.

Por tanto, el hecho de que los contenidos que un prestador del servicio transmite o almacena hayan sido proporcionados por terceros, es decir, que sean contenidos ajenos al prestador de servicios de intermediación, resulta básico desde el punto de vista de la exención de responsabilidad. En otro caso en que sea el propio prestador de servicios el responsable de la información almacenada o transmitida a través de la Red, las exenciones de responsabilidad no podrían aplicarse, y se acudiría a las reglas generales de responsabilidad civil, penal y administrativa establecidas en el ordenamiento jurídico español.

Las exenciones de responsabilidad que se establecen en la legislación comunitaria (en la DCE) y española (en la LSSICE) se pueden agrupar en tres categorías según sea la naturaleza de la actividad del prestador de servicios:

1- La prestación de servicios de mera transmisión de datos y de provisión de acceso a Internet.

2- La prestación del servicio de hosting o almacenamiento de datos[93].

3- La prestación del servicio de caching o servicio de realización y almacenamiento de copias.

Como puede verse, según sea la naturaleza de la actividad realizada por el prestador de servicios y no respecto a la condición del mismo, el prestador de servicios se podrá acoger a una exención de responsabilidad u otra según la categoría a la que pertenezca.

Puede pasar que el prestador del servicio no cumpla cada uno de los requisitos que se verán a continuación para cada una de estas categorías de exención y, por tanto, no se le pueda aplicar tal exención de responsabilidad; aunque esto no determina que se le atribuya responsabilidad, sino que no serían aplicables las exenciones de responsabilidad legisladoras, con lo cual para determinar su responsabilidad si la hubiere se procedería a analizar si en la actuación del prestador del servicio concurren los elementos exigidos por nuestro régimen general de responsabilidad. Pasemos a ver con detalle cada una de las categorías citadas anteriormente:

1- **Los servicios de mera transmisión de datos y de provisión de acceso a Internet**

Este primer supuesto de exención se establece en el párrafo primero del artículo 12 de la DCE, de donde se deduce que el prestador del servicio no podrá

[93] Se podría incluir un cuarto apartado que no es considerado en la directiva comunitaria DCE pero sí en la LSSICE, que es la responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (buscadores tipo Google, etc) , cuyas condiciones para la exención de responsabilidad, serán exactamente idénticas a las condiciones impuestas por la LSSICE para los prestadores de servicio de hosting o almacenamiento de datos

ser considerado responsable de los datos transmitidos cuando haya cumplido con los siguientes requisitos:

1- "*No haber originado él mismo la transmisión*", es decir, cuando el prestador no haya creado el contenido ni tampoco haya sido quien haya tomado la iniciativa de realizar la transmisión, convirtiéndose en simple ejecutor de la orden de envío de las comunicaciones comerciales, frecuentemente dada por el titular o anunciante de los bienes y servicios publicitados en la comunicación comercial.

2- "*No haber seleccionado al destinatario de la transmisión*", ya que si los prestadores eligen a los destinatarios de la transmisión ya no sería una simple actividad de intermediación, pasiva y automática, sino una acción activa y de control sobre uno de los elementos de la transmisión: los destinatarios.

3- "*No haber seleccionado ni modificado los datos transmitidos*", ya que si el prestador selecciona o modifica los datos transmitidos, entraría en una acción activa y de control sobre uno de los elementos de la transmisión (los datos transmitidos) y no pertenecería a la simple actividad de intermediación, pasiva y automática.

Esta exención de responsabilidad se recoge de forma idéntica en el artículo 14 de la LSSICE, exceptuando simplemente lo que **no** se entiende por "modificar la información": "*la manipulación estrictamente técnica de los archivos que alberguen los datos que tiene lugar durante su transmisión*".

Para que el prestador de servicios pueda acogerse a la exención de responsabilidad, debe cumplir los tres requisitos citados. Si no cumple algún requisito no se podrá aplicar la exención.

Es importante señalar la posibilidad de que un tribunal o una autoridad exijan al prestador de servicios que suspenda la transmisión de contenidos ilícitos, según indica el párrafo tercero del artículo 12 de la DCE. Si se produjera el supuesto señalado y se solicitara al prestador la finalización de su actuación,

el cumplimiento de dicha orden no se establece en el texto comunitario como requisito para gozar de la exención y, por tanto, el incumplimiento de la misma no implicaría la pérdida de la exención si se dan las condiciones establecidas anteriormente.

En cuanto a la legislación en España, la LSSICE en el párrafo primero del artículo 11 se contempla expresamente la posibilidad de que se pueda ordenar a los prestadores de servicios "*que suspendan la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio equivalente de intermediación que realizaran*", y, de modo general, para todos los servicios de intermediación "*Cuando un órgano competente por razón de la materia hubiera ordenado, en ejercicio de las funciones que legalmente tenga atribuidas, que se interrumpa la prestación de un servicio de la sociedad de la información o la retirada de determinados contenidos provenientes de prestadores establecidos en España, y para ello fuera necesaria la colaboración de los prestadores de servicios de intermediación*".

2- **La prestación del servicio de hosting**[94]

Se entiende por hosting aquel servicio de la Sociedad de la Información consistente en almacenar datos facilitados por el destinatario del servicio, es decir, aquellos prestadores de servicios de alojamiento o almacenamiento de datos.

Según se desprende del artículo 14 de la DCE, las condiciones que se deben cumplir para disfrutar de la exención de responsabilidad en la prestación del servicio de alojamiento son las siguientes:

1- Falta de conocimiento efectivo de la ilicitud de la actividad o de la información que se almacena, con carácter general para cualquier tipo de responsabilidad, tanto civil como penal.

[94] Los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (tipo Google), se acogerán a estas mismas condiciones para poder disfrutar de la exención de responsabilidad que recoge la LSSICE. Puede consultarse el artículo 17 de la citada ley para comprobarlo.

Para este punto, en la DCE no se especifica qué se entiende por "conocimiento efectivo", pero se deduce de la expresión que no basta con conocer efectivamente la existencia de una actividad o de unos datos, sino que además es necesario conocer la calificación jurídica ilícita de los mismos.

2- Actuar con prontitud para retirar los datos o para hacer que el acceso a ellos sea imposible en cuanto el prestador tenga conocimiento efectivo de la ilicitud, y en caso de una acción de daños y perjuicios, desde el mismo instante en que conoció hechos o circunstancias reveladores de la ilicitud.

Paralelamente, en la jurisprudencia española, el artículo 16 de la LSSICE incluye asimismo la citada exención de responsabilidad para los servicios de alojamiento o almacenamiento de datos, de forma idéntica a los empleados por la DCE, con la única diferencia de que sí especifica qué se entiende por el término "conocimiento efectivo", indicando que el mismo se da "*cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse*", es decir, cuando prestador tenga el conocimiento efectivo de que un órgano competente ha declarado la ilicitud de los datos o de la actividad, se ordene una retirada de los mismos o imposibilitar su acceso, y el prestador responsable de ello y con conocimiento de tal ilicitud, no los retire o no impida su acceso haciendo caso omiso de la resolución del órgano competente. Además dicho artículo de la LSSICE, añade el hecho de que el prestador no tenga conocimiento efectivo de que se ha producido lesión de bienes o de derechos de un tercero susceptibles de indemnización, para poder acogerse a la exención de responsabilidad.

Se puede deducir pues de tal artículo, que existen otros dos supuestos que pueden dar lugar, en su caso, a un resultado equivalente:

- "Los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios", es decir, procedimientos de detección y retirada que hayan sido pactados con entidades de gestión de derechos de propiedad, donde al prestador se le obligaría a retirar o imposibilitar el acceso al material ilícito, una vez cumplidos los requisitos de procedimiento consensuados.
- "Otros medios de conocimiento efectivo que pudieran establecerse", como, por ejemplo, códigos de conducta a los que se haya adherido el prestador y que deberán ser aceptados por quien proporciona contenidos (que es el cliente del prestador de servicios de almacenamiento), en la medida en que este deberá permitir al prestador la libre retirada de la información cuando, de conformidad con lo establecido en el código de conducta, resulte pertinente.

Hay que señalar que el anterior listado sirve de ejemplo y, en todos los casos, será el órgano judicial competente el que deberá calificar si el prestador tuvo o no un conocimiento efectivo de la ilicitud de la información o la actividad, haciendo uso de cualquier medio de prueba admitido en Derecho.

Para que sea aplicable la exención de responsabilidad del prestador de servicios de alojamiento, se requiere que los contenidos sean ajenos al prestador, según indican el artículo 14.2 de la DCE y el artículo 16.2 de la LSSICE, que establecen que cuando el destinatario del servicio actúa bajo la autoridad o el control del prestador de servicios, la exención de responsabilidad no le será de aplicación, ya que en este supuesto el prestador del servicio no actuaría como un mero intermediario.

Por último, añadir según indica el artículo 14.3 de la DCE, que la exención de responsabilidad para el prestador de servicio de alojamiento de datos "*no afectará a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exijan al prestador de servicios poner fin a una infracción o impedirla, ni a la posibilidad de que los Estados miembros establezcan procedimientos por los que se rija la retirada de datos o impida el acceso a ellos*". Es decir, si se ordena la retirada de determinada información o el bloqueo de la misma, su incumplimiento equivale a no cumplir con uno de los requisitos recogidos en los preceptos para el otorgamiento de la exención de responsabilidad, el de actuar "con prontitud para retirar los datos" o "hacer que el acceso a ellos sea imposible" y, en consecuencia, no se aplicará la exención de responsabilidad al prestador.

3- **La Prestación de servicios de caching de datos**

El denominado caching ó copia temporal de datos ó memoria tampón, se regula en el artículo 13 de la DCE y en el artículo 15 LSSICE, donde se exige a los Estados miembros que "*cuando se preste un servicio de la Sociedad de la Información consistente en transmitir por una red de comunicaciones datos facilitados por el destinatario del servicio, el prestador del servicio no pueda ser considerado responsable del almacenamiento automático, provisional y temporal de esta información, realizado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de éstos*"[95], siempre que el prestador de servicios cumpla con los siguientes requisitos:

- "*No modificar la información*".
- "*Cumplir las condiciones de acceso a la información*" a nivel comunitario y las condiciones impuestas a tal fin, por el destinatario cuya información se

[95] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información, en particular del comercio electrónico en el mercado. (Directiva sobre Comercio Electrónico). Artículo 13. Párrafo 1.

solicita a nivel nacional; es decir, el prestador del servicio que tiene una copia caché de un determinado sitio web debe exigir a los usuarios que le soliciten visitarlo las mismas condiciones que impone la web original.

-"*Cumplir las condiciones relativas a la actualización de la información*", con el objetivo de evitar que las copias en memoria caché queden obsoletas y muestren una información distinta de la que se ofrece en el sitio original que pueda producir daños y perjuicios.

- "*No interferir en la utilización lícita de tecnología ampliamente reconocida (generalmente aceptada) y utilizada por el sector con el fin de obtener datos sobre la utilización de la información*" en los ámbitos comunitario y estatal.

- "*Actuar con prontitud para retirar la información que haya almacenado, o hacer que el acceso a ella sea imposible, en cuanto tenga conocimiento efectivo del hecho de que la información ha sido retirada del lugar de la red en el que se encontraba inicialmente, de que se ha imposibilitado el acceso a dicha información o de que un tribunal o una autoridad administrativa ha ordenado retirarla o impedir que se acceda a ella*". Aquí se contempla el hecho de que el prestador, para poder acogerse a la exención de responsabilidad, asimismo ha de eliminar o impedir el acceso a la información cuando el lugar de red original ha retirado tal información (una especie de actualización en el borrado de la información), cuando el acceso a la información del lugar original se ha bloqueado, o por supuesto, cuando la autoridad competente ha determinado la ilicitud de tal información en cuyo caso dará lugar igualmente a su eliminación o bloqueo.

Por lo tanto, para que el prestador de servicios pueda gozar de la exención de responsabilidad, no basta únicamente con que la actividad coincida con la descrita en el supuesto de hecho, sino que además dependerá de que el prestador cumpla con todas las anteriores condiciones citadas que tanto la DCE como la LSSICE determina.

-Las obligaciones de supervisión y comunicación

Conforme con el párrafo primero del artículo 15 de la DCE, los estados miembros no pueden imponer a los prestadores de servicios una obligación general, ya sea de supervisar los datos que transmitan o almacenen, o bien de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas en relación a los servicios de alojamiento, tanto en los servicios de transmisión de datos, como en los de provisión de acceso a la Red, *caching* o *hosting*[96].

La Directiva comunitaria no sólo excluye la obligación de supervisión o control en términos generales, sino que incluso prohíbe la obligación de conservación o retención del tráfico de los datos. Por el contrario, en la legislación española, el artículo 12.1 de la LSSICE establece la obligación de los prestadores del servicio de retener los datos relativos a las comunicaciones electrónicas por un periodo máximo de 12 meses.

-LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y EL SPAM

Hasta esta parte del proyecto, se ha analizado el régimen jurídico de las comunicaciones comerciales, a partir de aquí se analizará en profundidad el mismo para que el proceso entero de envío de correos electrónicos comerciales no deseados se realice correctamente en cuanto a la obtención de los datos y al propio envío de ellos.

El envío de las comunicaciones comerciales depende, primeramente, de las condiciones en que las empresas hayan recopilado una serie de datos personales donde enviar tales comunicaciones en general y las direcciones de correo electrónico en particular (en este sentido, se pronuncia un Informe de 1999 de la Comisión Nacional de Informática y Libertades de Francia, que

[96] Sería igualmente extrapolable a los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda o comúnmente llamados "buscadores".

señalaba que el envío de mensajes electrónicos se basa en la recogida previa de direcciones electrónicas). Así mismo hay que recordar como ya se ha visto previamente en el presente proyecto, que como se desprende del artículo 19 de la LSSICE, es aplicable asimismo la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).

El derecho al tratamiento de datos de carácter personal implica el derecho fundamental a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, y que permite tener por nuestra parte el derecho de acceso, rectificación y cancelación de la información almacenada y disponer de los propios datos personales, tal y como lo reconoce el Tribunal Constitucional, en las STC 254/1993, de 9 de mayo (RTC 1993\254) o STC 11/1998, de 13 de enero (RTC 1998\11), entre otras. En la actualidad debe hablarse del derecho a la protección de datos de carácter personal, cuyo contenido será el mismo que se ha mencionado, ya que tras la entrada en vigor de la LOPD el ámbito de aplicación de este derecho, recogido en el artículo 2, se extiende a todos los datos de carácter personal registrados en soporte físico, es decir, tanto en soporte papel como en soporte informático o telemático (electrónico), siempre que sean susceptibles de tratamiento, quedando obsoleto, por tanto, el término "informática" que calificaba a esta pretendida libertad. Todo ello se verá a continuación, haciendo un análisis exhaustivo de la LOPD y las implicaciones que la misma conlleva en el envío de las comunicaciones comerciales no solicitadas, para que todo el proceso del mismo se realice acorde con la legalidad y la jurisprudencia vigente.

-Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)

Sujetos protegidos en la LOPD

La jurisprudencia española, concretamente en la LOPD, limita a las personas físicas la titularidad de la protección del derecho a la protección de datos de carácter personal, a diferencia de la LSSICE, que incluye tanto a personas físicas como jurídicas. Ello se pude desprender del artículo 1 de la citada ley que apunta lo siguiente: *"La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas* ***físicas****, y especialmente de su honor e intimidad personal y familiar*".

La exclusión de las personas jurídicas del amparo de este derecho, se puede deducir asimismo del artículo 3 en el párrafo a) de la LOPD, que establece la definición de "**datos de carácter personal**" (que son el objeto básico de protección en la mencionada ley) como "*cualquier información concerniente a personas* ***físicas*** *identificadas o identificables*", y del párrafo e) del citado artículo, en el que se considera como "**afectado o interesado**" a la "*persona* ***física*** *titular de los datos que sean objeto del tratamiento*".

En este mismo sentido se pronuncia la Agencia Española de Protección de Datos (AEPD), que en el Fundamento Jurídico II de la Resolución de 27 de febrero de 2001 afirma que "*… la protección conferida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, no es aplicable a las personas jurídicas, que no gozarán de ninguna de las garantías establecidas en la ley y, por extensión, lo mismo ocurrirá con los profesionales que organizan su actividad bajo la forma de empresa (ostentando, en consecuencia, la condición de comerciante a la que se refieren los artículos primero y siguientes del Código de Comercio) y con los empresarios individuales que ejercen una actividad comercial y respecto de los cuales sea posible diferenciar su actividad mercantil de su propia actividad privada, estando en el*

primer caso excluidos también del ámbito de aplicación de la Ley Orgánica 15/1999".

Según se desprende de lo anteriormente apuntado por la AEPD, se incluye pues en el concepto de personas físicas aquellos profesionales liberales que no tuvieran organizada su actividad profesional bajo la forma de empresa, es decir, que no posean la condición de comerciante (según el Código de Comercio), y los empresarios individuales cuando no fuera posible diferenciar su actividad mercantil de su propia actividad privada. Con lo cual, finalmente se excluyen del amparo de protección de la LOPD tanto a las personas jurídicas como a los profesionales y comerciantes individuales, cuando sus datos hayan sido tratados tan sólo en su consideración de empresarios.

Concepto de dato personal

Según se señala en la sección de definiciones del artículo 3 de la LOPD, en el párrafo a) de dicho artículo se define como "datos de carácter personal" a "*cualquier información concerniente a personas físicas identificadas o identificables*". Esta definición coincide con el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, de modo que el carácter personal del dato viene determinado por el hecho de ser concerniente a una persona física, no por ser un dato a través del cual se identifica a una persona. Es decir, lo relevante no es que el dato personal permita identificar a una persona, sino que dicha información debe estar referida o ser relativa a una persona física, quien puede estar identificada o ser identificable, según lo ha afirmado el Tribunal Constitucional en los fundamentos jurídicos sexto y séptimo de la Sentencia 292/2000, de 30 de noviembre.

Para aclarar el término "identificable" empleado en el anterior párrafo, podemos acudir a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos

datos. Concretamente, en el párrafo a) del artículo 2 se establece esa consideración de "identificable" (incluida en la definición de "datos personales") como la "*posibilidad de determinar, directa o indirectamente, la identidad de una persona mediante un número de identificación o uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*".

Para completar el concepto de dato personal, se puede consultar el párrafo 4 del artículo 1 del Real Decreto 1332/1994, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal; que define los "datos de carácter personal" de forma similar a las señaladas anteriormente, como "*toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión, concerniente a una persona física identificada o identificable*".

El problema en las definiciones de "dato personal" que se recogen tanto en la jurisprudencia española como en la comunitaria es que dicho término puede ser muy amplio y no es concreto, ya que dichas definiciones no permiten dar respuesta clara de qué datos concretamente se incluyen en la consideración de personales. Por ejemplo y relativa al fenómeno que se estudia en el presente proyecto, si la dirección de correo electrónico puede ser incluida en la expresión "dato personal". Por ello, se profundiza a continuación en dicho aspecto.

La dirección de correo electrónico como dato personal

Ha habido mucho debate en cuanto a la consideración de que la dirección de correo electrónico sea dato personal. Esto es cuestión muy importante a efectos de remitir comunicaciones comerciales no solicitadas, sobre todo en relación a aquellas direcciones que no aparecen vinculadas a la persona que la utiliza.

Repasando la definición de dato personal como cualquier información concerniente a personas físicas identificadas o identificables y teniendo en cuenta lo expuesto anteriormente, se pueden distinguir dos clases de direcciones de correo electrónico, atendiendo al grado de identificación que pueda tener la misma con el titular de la cuenta de correo:

- Aquellas en que voluntaria o involuntariamente la dirección de correo electrónico contenga información acerca de su titular, pudiendo aludir tanto a su nombre y apellidos como a la empresa en que trabaja o al país de residencia.

En este supuesto, la dirección de correo electrónico identifica al titular de la cuenta, por lo que tal dirección ha de ser considerada como dato de carácter personal. El modelo característico de este supuesto sería aquella dirección de correo electrónico en la que se hace constar el nombre y, en su caso, los apellidos del titular (o sus iniciales), correspondiéndose el dominio de primer nivel de la dirección de correo con el propio del país en que se lleva a cabo la actividad y el dominio de segundo nivel con la empresa en que se prestan los servicios, pudiendo de esta forma concretarse tanto la identificación de la persona como incluso el centro de trabajo al que pertenece.

- Aquellas en que, en principio, la dirección de correo electrónico no parece mostrar datos relacionados con el titular de la cuenta, como aquellas en las que la dirección está compuesta por una denominación abstracta o una simple combinación alfanumérica sin significado.

A priori podría afirmarse para este segundo supuesto, que este tipo de dirección de correo electrónico no es un dato de carácter personal. Sin embargo, incluso en este caso, en la dirección de correo electrónico aparecerá referenciado necesariamente un dominio de primer nivel, de forma que podrá procederse a la identificación del titular mediante la consulta del servidor en la que se gestione dicho dominio y aunque no lo parezca, dicha identificación no conlleva un gran esfuerzo según muestran los pronunciamientos tanto del

Grupo de Trabajo sobre Protección de Datos del artículo 29 de la Comisión en el documento de trabajo *"Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea*", de 21 de noviembre de 2000, como de la Agencia Española de Protección de Datos en su Memoria 1999. Además se puede desprender de ambos pronunciamientos que la dirección IP necesariamente vinculada a la dirección de correo electrónico también puede revelar datos personales del usuario, con lo cual a continuación se analiza asimismo en profundidad la posibilidad de que la dirección IP pueda ser un dato de carácter personal.

La dirección IP como dato personal

Para dar respuesta a esta cuestión se puede acudir al Informe 327/2003 elaborado por la Agencia Española de Protección de Datos, el cual señala que la dirección IP efectivamente sí es un dato de carácter personal. Este razonamiento parte del hecho de que los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables (que no requieren gran esfuerzo) a los usuarios de Internet a los que han asignado direcciones IP, y al poder ser identificable el cliente a partir de su dirección IP, ésta se considera un dato de carácter personal.

De hecho los proveedores de acceso a Internet normalmente tienen un fichero histórico de sus clientes en el cual se incluye la dirección IP (fija o dinámica) asignada, el número de identificación del abonado, la fecha, la hora y la duración de la asignación de dirección IP. Con lo cual, a través de terceros que son los responsables de la asignación de la dirección IP, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil (nombre, dirección, número de teléfono, etcétera), por medios razonables (no costosos). Tal posibilidad de identificación del usuario a partir de su dirección IP hace que la misma sea un dato de carácter personal, como marca la LOPD en el párrafo a) del artículo 3 de la LOPD.

Concluyendo, tanto la dirección IP como la dirección de correo electrónico en cualquiera de sus formas, es un conjunto de datos personales del usuario y como tal, está acogido por el amparo de la LOPD.

El consentimiento del titular de los datos

De forma similar a la legalidad en el envío de las comunicaciones comerciales no solicitadas, en las cuales es necesaria la obtención del consentimiento del destinatario, la regla general en materia de tratamiento de datos personales es la exigencia obtener el consentimiento inequívoco de aquel individuo sobre el que se realizará un tratamiento de sus datos.

Y así, la LOPD en el párrafo h) del artículo 3 define el "consentimiento del interesado" como "*toda manifestación de voluntad, libre, inequívoca, específica e informada mediante la que consiente en el tratamiento de datos que le conciernen*". Además la citada ley en sus artículos 6 (consentimiento del afectado) y 7 (datos especialmente protegidos) establece tres formas de obtener el consentimiento del afectado para el tratamiento de sus datos, según a qué clase de datos de carácter personal se haga referencia en dicho tratamiento:

- Para la obtención y tratamiento de datos de carácter personal "*se requerirá el consentimiento inequívoco del titular de los datos salvo que la ley disponga otra cosa*".[97]

- Para el tratamiento de datos de carácter personal relacionados con las creencias, ideología o religión, se requerirá que el titular de los mismos otorgue su "*consentimiento expreso y* ***por escrito*****"** para que puedan ser tratados. [98]

- Para "*los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos*

[97] Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos. Artículo 6. Párrafo 1.
[98] Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos. Artículo 7. Párrafo 2.

cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente".[99]

En este contexto, la dirección de correo electrónico es un dato de carácter personal que no hace referencia en principio a las creencias, ideología, religión, origen racial, salud ni a la vida sexual del titular. Por ello, únicamente es necesario el consentimiento inequívoco del afectado para realizar el tratamiento en este caso de su correo electrónico.

Al igual que en ocurre en el caso del consentimiento del destinatario en el envío de comunicaciones comerciales no solicitadas que marca la LSSICE, la LOPD asimismo se refiere únicamente al concepto de "consentimiento inequívoco", por lo que se incluye en dicho concepto no sólo el consentimiento expreso sino también el consentimiento tácito, como se da en la LSSICE, siempre y cuando se otorgue al afectado un plazo prudencial para que pueda tener claramente conocimiento de su omisión de oponerse al tratamiento de sus datos.

Hay que señalar que como se indica en el párrafo 3 del artículo 6 de la LOPD, el consentimiento "*podrá ser revocado cuando exista causa justificada para ello* y no se le atribuyan efectos retroactivos", es decir, cuando exista una quiebra de la confianza entre el afectado y el responsable del fichero, con lo que se podría solicitar la cesación del tratamiento de datos con la simple alusión a la voluntad de preservar su derecho a la intimidad.

Excepciones al consentimiento

Existe una serie de casos, en los que hay una excepción del régimen general del consentimiento del titular de los datos personales. Son los siguientes:

a) Cuando los datos personales se recojan para el ejercicio de las funciones propias de las administraciones públicas en el ámbito de sus competencias.

[99] Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos. Artículo 7. Párrafo 3.

b) Cuando los datos personales se refieran a las partes de un contrato o precontrato de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.

c) Cuando el tratamiento de los datos especialmente protegidos resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto o cuando el tratamiento tenga por finalidad proteger el interés vital del interesado en el supuesto de que esté física o jurídicamente incapacitado para dar su consentimiento.

d) Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos.

En cuanto a la última excepción del régimen general del consentimiento del titular de los datos personales hay que señalar que los remitentes de comunicaciones comerciales no solicitadas suelen obtener los datos personales de fuentes accesibles al público.

Se define el término "fuentes accesibles al público" en el artículo 3 párrafo j) de la LOPD, como "*aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación*" y estos consisten exclusivamente en "*el censo promocional, los repertorios telefónicos en los términos previstos regulados, las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, actividad, grado académico, dirección e indicación de su pertenencia al grupo, los diarios y boletines oficiales y medios de comunicación*".

Falta establecer si esta lista que establece la LOPD como medios accesibles al público es una lista *numerus clausus* o *numerus apertus*, es decir, es una lista cerrada en la cual no cabe ningún otro tipo de medio accesible al público o es simplemente una enumeración exhaustiva en la que se puede incluir a tal efecto otra fuente de acceso, ya que el entorno de Internet se ha convertido en la mayor base de datos de carácter personal.

En un principio, ya que Internet es considerado un medio de comunicación en el que se almacenan múltiples informaciones y de acceso libre a todos los usuarios conectados a la Red, se podría pensar que la recopilación de direcciones de correo electrónico sin necesidad de recabar el consentimiento del afectado estaría permitido. Pero contrariamente a esta idea, la Agencia Española de Protección de Datos en el Informe del año 2000 afirma que no considera que la procedencia de los datos recogidos en Internet sea la de fuente accesible al público, siendo necesario, por lo tanto, la obtención del consentimiento inequívoco, específico e informado del afectado para realizar tratamientos con los datos personales publicados en Internet, aunque estos se hayan publicado de forma que cualquier usuario de Internet pueda acceder a los mismos.

Por ello hay que destacar que el carácter de fuente accesible tiene una serie de limitaciones, según indica el artículo 28 de la LOPD en su párrafo tercero: "*cuando los datos aparezcan editados en forma de libro u otro soporte físico la nueva edición hará decaer el mismo, y en el caso de que se obtenga copia de la lista en formato electrónico, esta perderá el carácter de fuente accesible al público en el plazo de un año contando desde el momento de la obtención*".
Igualmente, cuando pase un año de la recolección del listado de datos recogidos en el censo promocional, la lista perderá su carácter de fuente de acceso público según se indica en el párrafo segundo del artículo 31 de la LOPD, con lo que el uso de cada lista de censo promocional tendrá un plazo de vigencia de un año.

Aun suponiendo que Internet tiene la consideración de fuente accesible al público, es necesario para que se dé el caso de la excepción del consentimiento, que dicho tratamiento de datos sea necesario para satisfacer el interés legítimo perseguido por el responsable del fichero o por el tercero a quien se comuniquen los datos. Con lo cual sería cuestionable si como interés legitimo puede entenderse el envío de publicidad, promociones u ofertas.

Es importante destacar que contrariamente al consentimiento, o en contraposición a la excepción del consentimiento del mismo, en el párrafo cuarto del artículo 6 de la LOPD se recoge que "*en los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado*". De ello se desprende el **derecho de oposición**, que consiste en la negativa a la continuación del tratamiento de los datos, es decir, la cancelación genérica respecto de todos los datos que pudieran estar sometidos al tratamiento de los mismos.

En este mismo sentido, se puede acudir al artículo 30 de la LOPD en su párrafo cuarto, que contempla el derecho de oposición, pero respecto de los tratamientos de datos con fines de prospección comercial y publicidad directa, que indica que los "*interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud*".

Relativo a este último punto faltaría establecer cuál es el plazo de validez de la oposición del consumidor al tratamiento de sus datos, es decir, hasta cuándo

debe entenderse vigente esa manifestación de oposición al tratamiento y de exclusión a aparecer en las fuentes accesibles al público. Mayoritariamente se entiende que con la actualización del censo o la publicación de una nueva guía caduca la manifestación de oposición emitida.

El régimen del consentimiento para la cesión de datos personales

La LOPD en el párrafo i) del artículo 3 define la **cesión o comunicación de datos** como "*toda revelación de datos realizada a una persona distinta del interesado*".

Como norma general, el artículo 11 de la LOPD establece en la cesión de datos la necesidad de obtener el consentimiento del interesado, al igual que sucedía para el tratamiento de datos personales.

Dicho consentimiento, al igual que en el caso del tratamiento de datos, tiene un carácter revocable, aunque en este caso no se exige la concurrencia de causa justificada.

Se establece, asimismo, que será considerado **nulo** el consentimiento prestado para la cesión o comunicación, según indica el artículo 11 de la LOPD en su tercer párrafo, "*cuando la información que se facilite al interesado no le permita conocer la **finalidad** a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien pretende comunicar*".

Esta norma general del previo consentimiento del interesado para la cesión de sus datos personales no se aplicará en los siguientes casos[100]:

- Cuando la cesión esté autorizada en una ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público.
- Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso, la comunicación sólo será legítima en cuanto se limite a la

[100] Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos. Artículo 11. Párrafo 2.

finalidad que la justifique, lo que debe interpretarse en sentido estricto o restringido y no permitir otras cesiones que las estrictamente necesarias para la ejecución de lo contratado.

- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los jueces o tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas, o a instituciones autonómicas análogas al Defensor del Pueblo o al Tribunal de Cuentas.
- Cuando la cesión se produzca entre administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
- Cuando la cesión de datos personales relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

El derecho de la información en la recogida de datos

El derecho de información en la recogida de datos se recoge en el artículo 5 de la LOPD, y genéricamente consiste en que "*los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco*". Aunque el caso varía dependiendo de la modalidad de recogida de los datos como se puede ver a continuación:

Modalidad directa de obtención de datos

Esta modalidad consiste en obtener la dirección de correo electrónico del propio titular, en cuyo caso "*los interesados a los que soliciten datos personales deberán ser previamente informados, de modo expreso, preciso e inequívoco de las siguientes cuestiones*":

- De la existencia de un fichero o tratamiento de datos de carácter personal, y de los destinatarios de la información.
- De la finalidad de la recogida de los datos, puesto que los mismos deben ser "adecuados, pertinentes y no excesivos" en función de la finalidad o finalidades para los que se han obtenido. Además, se exige una compatibilidad entre los fines para los que los datos fueron recogidos y los fines a los que efectivamente se destina su tratamiento, ya que si se quisiera utilizar un determinado dato con una finalidad distinta para la que se hubiera obtenido, sería necesario contar de nuevo con el requisito de la obtención del consentimiento.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, oposición y rectificación y cancelación.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Acudiendo a la sección de definiciones de la LOPD en su artículo 3, párrafo d), el "responsable del fichero o tratamiento" es la "*persona física o jurídica, de naturaleza pública o privada u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento*".

Además de los preceptos anteriores, cuando la recogida de los datos personales sea a través de Internet, deberá constar el código de inscripción asignado por el Registro General de Protección de Datos con el fin de asegurar el conocimiento del interesado de la posibilidad de ejercitar los derechos de acceso, cancelación y modificación, de conformidad con las recomendaciones

de la Agencia de Protección de Datos al sector del comercio electrónico, para la adecuación de su funcionamiento a la LOPD.

En cuanto a la manera de facilitar la citada información, la ley es tajante en este aspecto. Conforme con el artículo 5 de la LOPD, los interesados a los que se soliciten datos personales deberán estar previamente informados de modo expreso, preciso e inequívoco, por lo que dicha información deberá ser perfectamente visible en el proceso de recogida de los datos. Teniendo en cuenta los distintos métodos de recogida de los mismos:

- Si se utilizan cuestionarios u otros impresos para la recogida de los datos figurarán en los mismos, en forma claramente legible, los preceptos anteriormente detallados.
- Si los datos se recogen a través de una página web, deberá hacerse expresa referencia a estas cuestiones en el formulario correspondiente, no bastando la simple inclusión de esta información en un aviso legal o política de privacidad ubicado en otra página distinta dentro del sitio web, ni la mera mención en las cláusulas adicionales a las condiciones generales que rigen la vinculación del vendedor con el comprador al hecho de que los datos que se faciliten serán protegidos de acuerdo a la ley. Aun así, la Agencia Española de Protección de Datos, en su Memoria de 2001, señala que cabe la posibilidad de obtener dicha información a la que se ha hecho referencia mediante un clic en un botón adecuadamente etiquetado, aunque no se considere la opción más adecuada.

Hay que destacar relativo a este punto que según indica el párrafo 3 del artículo 5 de la LOPD, "*no será necesario contemplar el carácter obligatorio o facultativo de su respuesta a las preguntas que son planteadas, las consecuencias de la obtención de los datos o de la negativa a suministrarlos y la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y*

oposición, si del contenido de la misma se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban".

Modalidad indirecta de obtención de datos

En esta modalidad, los datos de carácter personal no han sido recogidos del interesado, sino que se han obtenido de otra empresa por cesión de datos o por otra persona.

Este caso es comprendido por el párrafo cuarto del artículo 5 de la LOPD, que establece la obligación del responsable del fichero o su representante de informar de forma expresa, precisa e inequívoca al interesado de los preceptos que contempla el derecho de información, que se han detallado anteriormente en el apartado de "Modalidad directa de obtención de datos", dentro de los tres meses siguientes al momento del registro de los datos. Esto supone que necesariamente el remitente debe ponerse en contacto con los futuros destinatarios de comunicaciones comerciales para cumplir estos requisitos, aunque sea a través del correo electrónico.

Se exime de esta obligación al responsable del fichero cuando el interesado ya hubiera sido informado con anterioridad del contenido del tratamiento de la procedencia de dichos datos, de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de estos, de los destinatarios de la información, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición y de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Obtención de datos de fuentes accesibles al público

El último caso es cuando los datos personales (por ejemplo la dirección de correo electrónico) se obtienen por fuentes accesibles al público y son destinados a actividades de publicidad o prospección comercial. En este caso, en

cada comunicación que se dirija al interesado se le informará del origen de los datos, de la identidad del responsable del tratamiento y de los derechos de acceso, cancelación, rectificación y oposición a los mismos que tiene a su disposición el mismo[101].

La cesación del deber de información se justifica en estos supuestos, ya que el interesado tiene la oportunidad de oponerse a la inclusión de forma genérica según se dispone en el artículo 28 de la LOPD, que indica que "*los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes*". Del mismo modo, "*los profesionales que constan en las guías elaboradas por los colegios profesionales tienen derecho a que la entidad responsable del mantenimiento de los listados indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial*".

Asimismo sobre este aspecto podemos acudir a la legislación europea, concretamente a la Directiva 95/46/CE sobre protección de datos personales y su libre circulación, que declara ilegal la práctica de la recogida de datos personales(como direcciones de correo electrónico) en sitios web de forma automática o no automática.

Y es que la protección de datos constituye en principio importante para la Unión Europea, podemos observarlo en el Tratado de la Unión Europea, concretamente en sus artículos 6 (derecho de los principios de libertad, democracia y respeto de los derechos humanos y libertades fundamentales) y 30 (exige la sujeción de la recogida, el almacenamiento, tratamiento, análisis e intercambio de información en el ámbito de la cooperación policial a las disposiciones correspondientes en materia de protección de datos personales), en la Carta de los Derechos Fundamentales en su artículo 8 (la protección de los

[101] Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos. Artículo 5. Párrafo 5.

datos personales constituye una de las libertades enunciadas) y como hemos visto en la Directiva 95/46/CE, que invita a los estados miembros a garantizar los derechos y libertades de las personas físicas en lo referido al tratamiento de sus datos personales, especialmente a su derecho a la intimidad de forma que estos datos puedan circular libremente por la Unión Europea, velando por los derechos y libertades de las personas en materia de tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento, principios que comparte la Directiva Europea en su mayoría con la LOPD española, basados en la calidad de los datos recogidos, legitimación del tratamiento de los datos, confidencialidad y seguridad de dicho tratamiento, consentimiento inequívoco del titular de los datos, derechos del interesado (titular de los datos) de información, acceso, oposición, rectificación, etc. que en su contenido son similares a los principios incluidos en la LOPD.

Esta Directiva general sobre la protección de datos está complementada por la Directiva sobre la privacidad en las comunicaciones electrónicas disponibles para el público en las redes de comunicación pública.

Asimismo existen otras Directivas en la Comunidad Europea en materia de tratamiento de datos personales, como la Directiva 97/66/CE que transforma los principios establecidos en la anterior Directiva comentada (95/46/CE), en normas concretas para el sector de telecomunicaciones, y la Directiva 2002/58/CE, que deroga la anterior Directiva para adaptarla al desarrollo de los mercados y las tecnologías de los servicios de las comunicaciones electrónicas con el fin de que el nivel de protección de los datos personales ofrecido a los usuarios de los servicios de comunicaciones electrónicas sea el mismo con independencia de la tecnología empleada. Finalmente ésta fue a su vez modificada por la Directiva 2006/24/CE relativa a la conservación de datos personales en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de telecomunicaciones.

El marco legislativo de la Comunidad Europea sobre protección de datos y privacidad, fue establecido con el fin de que la innovación tecnológica no lo dejara obsoleto y fuera eficaz para la preservación de derechos y libertades en las sociedades tecnológicas dependientes del uso de las TIC, evitando en la medida de lo posible los riesgos de seguridad en el tráfico de datos personales en la Red y velando por los derechos de los interesados y sus intereses legítimos. Aunque las autoridades encargadas de ello se enfrentan a grandes desafíos derivados de los constantes cambios tecnológicos, que se adelantan a la evolución de las normas legales que lo regulan. Asimismo resulta difícil su control debido a la globalización de los datos y el hecho de la extraterritorialidad en la aplicación de las normas.

Finalmente en la legislación española, se puede acudir también a la Ley 32/2003 General de Telecomunicaciones, que en el párrafo 6 de su artículo 38, establece que "*en la elaboración y comercialización de las guías de abonados a los servicios de comunicaciones electrónicas y la prestación de los servicios de información se garantizará, en todo caso, a los abonados el derecho a la protección de sus datos personales, incluyendo el de no figurar en dichas guías*", estableciendo un paralelismo de semejanza con la Ley de Protección de Datos de Carácter Personal.

Régimen sancionador de la LOPD

Primeramente identificar a los sujetos a los cuales será de aplicación el régimen sancionador de la LOPD. Para ello, acudimos al artículo 43 de la LOPD que establece que estarán sujetos al régimen sancionador de la susodicha ley "*los responsables de los ficheros y los encargados de los tratamientos*".

Las infracciones, de la misma forma que establecía la LSSICE, se calificarán como leves, graves o muy graves, según apunta el artículo 44 de la LOPD. El

establecimiento del tipo de infracción cometida atiende a las siguientes condiciones para cada uno de los tipos:

Infracciones leves:

Son infracciones leves aquellas que cumplan cualquiera de las siguientes condiciones:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 LOPD.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley (obligación por parte del responsable del fichero y quienes intervengan en cualquier fase del tratamiento del deber de guardar el secreto profesional respecto de los datos tratados) salvo que constituya infracción grave.

Infracciones graves:

Son infracciones graves aquellas que cumplan cualquiera de las siguientes condiciones:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el "Boletín Oficial del Estado" o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) Impedir u obstaculizar el ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

Infracciones muy graves:

Son infracciones muy graves aquellas que cumplan cualquiera de las siguientes condiciones:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática, el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Las infracciones anteriormente descritas que la ley tipifica prescriben por el transcurso de un año las leves, dos años las graves y tres años las muy graves, que comenzarán a contar desde el día en que se cometió la infracción[102].

Asimismo, según se indica en el mismo artículo, "*se interrumpirá la prescripción con la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviera paralizado durante más de seis meses por causa no imputable al presunto infractor*".

Sanciones

En cuanto a la cuantía de las sanciones, el artículo 45 de la presente Ley fija las sanciones que corresponden a las infracciones cometidas:

Las infracciones leves serán sancionadas con multa de 601,01 a 60.101,21 euros, las infracciones graves serán sancionadas con multa de 60.101,21 a 300.506,05 euros y las infracciones muy graves serán sancionadas con multa de 300.506,05 a 601.012,10 euros.

[102] Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos. Artículo 47. Párrafo 1.

La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

Si en razón de las circunstancias concurrentes se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

En ningún caso podrá imponerse una sanción más grave que la fijada en la ley para la clase de infracción en la que se integre la que se pretenda sancionar.

Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años, y las impuestas por faltas leves al año [103].

El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquél en que adquiera firmeza la resolución por la que se impone la sanción[104].

Las resoluciones de la Agencia Española de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa[105] y sólo serán susceptibles de impugnación en la jurisdicción contencioso-administrativa.

Destacar finalmente a efectos de responsabilidad, que la normativa de protección de datos señala que ostentará la condición jurídica de responsable del fichero aquél que decide los fines y medios del tratamiento de los datos

[103] Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos. Artículo 47. Párrafo 4.
[104] Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos. Artículo 47. Párrafo 5.
[105] Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos. Artículo 48. Párrafo 2.

personales, bien sea una sola persona física individual o conjunta siendo varios los responsables o incluso entidades, mientras que el proveedor de servicios será el que realiza el tratamiento por cuenta del responsable del fichero y de acuerdo con sus instrucciones. La relación entre ambas figuras se regula en el contrato; en él se establecerá que el encargado del tratamiento se obliga a tratar los datos según las instrucciones del responsable del fichero, que no comunicará los datos a terceros, que no los usará con fin distinto al pactado y que los destruirá o devolverá una vez finalizada la relación contractual. Asimismo, deberán fijarse las medidas de seguridad de índole técnica y organizativa que aplicará el encargado del tratamiento a los ficheros. Por todo, será la precisa y correcta redacción de los términos del contrato la determinante para la delimitación de eventuales responsabilidades entre las partes, y para la consiguiente aplicación del régimen sancionador establecido en la LOPD, en caso de ser necesario.

Problemática de la doble imposición de sanciones

Puede darse el caso de que el envío de correos electrónicos comerciales no deseados sean susceptibles de cometer infracciones tanto de la LOPD como de la LSSICE, y en consecuencia llevar implicada una doble imposición de sanciones, una por cada ley de las mencionadas.

En este punto cabe destacar que la tradición jurídica en el Derecho español prohíbe este caso.

Por ello, se debe plantear la situación de que una infracción de la LSSICE en materia de comunicaciones comerciales pueda teóricamente coincidir con el mismo hecho que esté también sancionado por la LOPD, llevando a la doble imposición de la sanción.

Para resolver esta situación es necesario acudir a las infracciones contenidas en la LSSICE para observar si alguna de ellas tiene su correspondiente sanción en la LOPD y, en este caso, cómo se resolvería la doble regulación.

Lo que sí está claro, es que existen algunas obligaciones que hay que cumplir en la LSSICE que no tienen su equivalente en la LOPD y, por lo tanto, las sanciones que se impongan por estas causas difícilmente pueden incurrir en el caso de la doble imposición de sanción. Algunos ejemplos de este caso pueden ser la identificación de los mensajes comerciales, la indicación de la persona física o jurídica en nombre de quien se envían estos o la transparencia en las ofertas promocionales.

El mayor problema en este caso radica en el supuesto de que el prestador de servicios hubiera enviado un correo electrónico sin haber recabado anteriormente el consentimiento expreso del destinatario, infringiendo, por tanto, el artículo 21de la LSSICE, y, además, hubiera infringido la LOPD por haber obtenido la dirección de correo de forma antijurídica.

Pues bien, para este caso se considera que se trata de infracciones diferentes, puesto que la LSSICE y la LOPD tienen ámbitos de aplicación diferentes, aunque ciertamente interrelacionados, y, en consecuencia, cabría una sanción conforme a la LSSICE por lo que respecta al envío de correos comerciales no solicitados o autorizados expresamente y una segunda sanción conforme a la LOPD por lo que respecta a la infracción cometida al obtener los datos de una fuente ilegítima.

En el resto de casos en los que se pudiera pensar en hipotéticas colusiones reales de infracciones, deberían dirimirse las mismas teniendo muy presentes los principios generales del Derecho, como el principio de especialidad, optando por la aplicación de la LSSICE cuando la infracción se refiera expresamente a un correo electrónico.

Acción de cesación

Como se visto anteriormente en otros apartados, concretamente en el artículo 19 de la LSSICE, se hace remisión expresa a la normativa de publicidad. Acudiendo al artículo 2 de la Ley General de Publicidad, se define la “publicidad”

como "*toda forma de comunicación realizada por una persona física o jurídica, pública o privada, en el ejercicio de una actividad comercial, artesanal o profesional, con el fin de promover de forma directa o indirecta la contratación de muebles o inmuebles, servicios, derechos y obligaciones*" y considera "**ilícita**" a "*la publicidad que atente contra la dignidad de la persona o vulnere los valores o derechos reconocidos en la Constitución*...", como indica el artículo 3 párrafo a) de la citada Ley, con lo que se podría afirmar, por los motivos anteriormente expuestos, que las comunicaciones comerciales no solicitadas constituyen "publicidad ilícita".

Con lo cual, en un principio, serían ejercitables las acciones de cesación y rectificación y el ejercicio de las acciones civiles, administrativas, penales o de otro orden que correspondan y con la persecución y sanción como fraude de la publicidad engañosa por los órganos administrativos competentes en materia de protección y defensa de los consumidores y usuarios, según indica el artículo 32 de la LGP. Aunque a continuación veremos que este hecho se verá matizado de forma importante según se desprende de la citada Ley.

Concretamente, la LGP establece que cualquier persona natural o jurídica que resulte afectada y, en general, quienes tengan un derecho subjetivo o un interés legítimo, podrán solicitar del anunciante la cesación o, en su caso, la rectificación de la publicidad ilícita, es decir, el ejercicio de las acciones de cesación y de rectificación.

Los amplios términos en los que se pronuncia el artículo 25 de la LGP al reconocer legitimación activa, para el ejercicio de las acciones de cesación y rectificación, tanto a órganos administrativos como a las asociaciones de consumidores, a las entidades de otros Estados miembros de la Comunidad Europea (las cuales deberán estar constituidas para la protección de los intereses colectivos y de los intereses difusos de los consumidores que estén habilitadas mediante su inclusión en la lista publicada a tal fin en el Diario Oficial de las Comunidades Europeas) y, en general, a quien tenga un derecho

subjetivo o interés legítimo, **no permiten**, sin embargo, que pueda pensarse que las empresas competidoras del sector puedan actuar contra quien remite este tipo de publicidad ilícita (las comunicaciones comerciales no solicitadas) **a no ser que se acredite el perjuicio directo** que para ellas hayan supuesto esas actuaciones infractoras.

El objeto de actuación de la presentación de estas acciones, como su propio nombre indica, es la cesación de la conducta contraria a la presente Ley y la prohibición de una reiteración futura. Asimismo, la acción podrá ejercerse para prohibir la realización de una conducta cuando esta haya finalizado al tiempo de ejercitar la acción, si existen indicios suficientes que hagan temer su reiteración de modo inmediato, según indica el párrafo segundo del artículo 29 de la LGP.

La solicitud de estas acciones, tal y como lo establece el párrafo tercero del artículo 25 de la citada Ley, se hará por escrito, en forma que permita tener constancia fehaciente de su fecha, de su recepción y de su contenido.

En cuanto a los plazos de ejercicio de las citadas acciones, el párrafo primero del artículo 26 de la LGP establece que la cesación podrá ser solicitada desde el comienzo hasta el fin de la actividad publicitaria, mientras que la rectificación, según el párrafo primero del artículo 27 de la misma Ley, podrá solicitarse desde el inicio de la actividad publicitaria hasta siete días después de finalizada la misma.

5- Cuestiones deontológicas relacionadas con el Spam

Este apartado del proyecto ha sido elaborado consultando el proyecto final de carrera[106] de idéntica temática del año anterior, añadiendo información citada encontrada en otros medios y comentarios propios.

El problema derivado del spam, es que en Internet hay una ausencia de una regulación internacional unificada. Además, tal y como viene expuesto en la LSSICE, la implantación de Internet tropieza con algunas incertidumbres jurídicas que es necesario aclarar mediante el establecimiento de un marco jurídico adecuado que genere en todos los actores implicados la confianza necesaria para el empleo de este nuevo medio.

Esto ha provocado que la regulación de la publicidad en Internet plantee por un lado problemas de jurisdicción competente y aplicable y por otro lado la dificultad de someter a control las conductas ilícitas en publicidad por las distintas normativas de aplicación a nivel comunitario y extracomunitario. Esta ausencia de legislación única aplicable al entorno de Internet ha impulsado a las instituciones europeas a legislar y cooperar internacionalmente con el fin de asumir principios generales sobre el comercio electrónico y la publicidad.

En el ámbito comunitario se cuenta con una normativa específica. En el español, como ya hemos visto se cuenta con leyes y códigos éticos de buenas prácticas que regulan los servicios de la sociedad de la información y el comercio electrónico junto a las especificaciones de la publicidad para el nuevo medio electrónico.

Es importante destacar que según el orden de preferencia jerárquica de las normas, en principio, deben aplicarse y tienen eficacia directa los Convenios Internacionales suscritos por España. A falta de que se apruebe un acuerdo que regule el comercio electrónico o Internet en general, se aplican los convenios existentes en materia civil, mercantil y penal.

[106] Álvarez (2010)

Asimismo la Constitución Española impone la integración en el ordenamiento jurídico interno de las normas emanadas de las instituciones comunitarias. En este sentido las Directivas europeas han regulado las comunicaciones comerciales surgidas en el nuevo entorno electrónico.

Además de las Directivas y, con igual carácter vinculante, se han redactado numerosos reglamentos, decisiones comunitarias, comunicaciones y dictámenes que no se imponen de forma obligatoria, sobre la regulación de materias relacionadas con Internet. El problema de estos textos comunitarios es que aunque son de obligado cumplimiento, son normas de mínimos por lo que su adecuación a los distintos ordenamientos jurídicos de los estados miembros no es homogénea. Finalmente se cuenta con la cooperación internacional y la autorregulación.

La problemática derivada de la generalización del uso de Internet como vía comercial y medio de difusión publicitario y de apertura al mercado de las telecomunicaciones se ha tenido en cuenta desde diversos organismos internacionales, por ello se han dictado a modo de recomendaciones una serie de pautas o principios generales relativos al comercio electrónico que afectan a la publicidad y las ofertas comerciales difundidas por la Red y que han servido de guía para posteriores redacciones de códigos deontológicos o de buenas prácticas.

Asimismo ha sido necesario un marco regulador de las comunicaciones electrónicas para reforzar su competencia, facilitar la entrada en el mercado a nuevos operadores, estimular la inversión y hacer más competitivo el sector. Este marco regulador de las comunicaciones electrónicas viene comprendido en la **Directiva 2002/21/CE** relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas o “Directiva Marco”.

Este marco regulador de las redes y los servicios de comunicaciones electrónicas forma parte del paquete de Directivas que regulan las

comunicaciones electrónicas en la Unión Europea. Este paquete está formado por las siguientes directivas:

-**Directiva Marco**[107]: establece el marco regulador común a todas las redes y servicios de comunicaciones así como los recursos asociados a ellos.

-**Directiva de autorización**[108]: garantiza la libertad de suministrar redes y servicios de comunicaciones electrónicos.

-**Directiva de servicio universal**[109]: establece el conjunto mínimo de servicios de calidad especificada al que todos los usuarios finales tienen acceso, teniendo en cuenta las condiciones nacionales específicas, a un precio asequible sin distorsión de la competencia.

-**Directiva de acceso**[110]: establece un marco regulador para las relaciones entre suministradores de redes y servicios compatible con los principios de mercado interior y que garantice la interoperabilidad de los servicios de comunicación electrónica y redunde en beneficio de los consumidores.

-**Directiva sobre privacidad y comunicaciones electrónicas**[111]: garantiza un nivel equivalente de protección de las libertades y los derechos fundamentales y concretamente el derecho a la intimidad en el tratamiento de datos personales y su libre circulación en el sector de las comunicaciones electrónicas.

Los sistemas de control de las comunicaciones comerciales no consentidas bien se relegan a la autorregulación cuyos principios y normas son recogidos en códigos éticos o de conducta o bien son regulados por normativa legal.

---

[107] Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva Marco).

[108] Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización).

[109] Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).

[110] Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso).

[111] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Hay básicamente dos sistemas para la regulación del spam, el primero exige el consentimiento expreso del receptor de correos electrónicos autorizando su envío, es el sistema de **listas de exclusión opt-out**, en el que se da el envío no autorizado de mensajes comerciales a una lista de correo electrónico de internautas que no han dado consentimiento explícito a la recepción de tales mensajes, pero con posibilidad de que los afectados se puedan retirar de la lista. Es un sistema de acuerdo implícito del afectado (mientras el afectado no se retire de la lista, por defecto se le pueden mandar correos electrónicos no solicitados). Como en este sistema para no recibir correo comercial el afectado tiene que incluirse en la lista para excluirlo del envío, y normalmente los usuarios no suelen hacerlo, este sistema implica un número potencial de destinatarios mayor y beneficia al anunciante o remitente de dichos correos comerciales.

El segundo sistema permite el envío al destinatario siempre que éste haya manifestado previamente la voluntad expresa de recibirlo, este sistema es de **listas de inclusión opt-in**. A diferencia del anterior, este sistema exige un acuerdo explícito del afectado.

Periódicamente las empresas que envían comunicaciones comerciales deben revisar dichas listas para actualizar posibles bajas/altas en las listas y evitar el envío en los casos denegados legalmente.

La elección de uno u otro sistema va en función de la política legislativa y la presión ejercía por grupos con intereses en juego[112].

Existen partidarios del sistema de listas de exclusión voluntaria que defienden que el derecho de oposición debe ejercerse únicamente frente al remitente del mensaje no solicitado. Por otro lado se encuentran los partidarios de mecanismos de listas de exclusión, nacionales o internacionales, en el que

[112] Aparicio (2005).

pueda inscribirse quien lo desee, antes o después de haber recibido mensajes no solicitados, en cuyo caso deben ser los responsables de los envíos quienes deben consultar regularmente dichas listas con el fin de respetar el deseo expreso manifestado por los usuarios inscritos en ellas[113].

La elaboración de dichas listas puede ser realizada de dos formas. La primera a partir de listas públicas a nivel nacional (en este caso el usuario deberá inscribirse en una sola lista) y la segunda a partir de listas privadas múltiples (el usuario deberá inscribirse en todas las listas manifestando el rechazo a recibir comunicaciones comerciales no solicitadas para lograr tal efecto).

Este sistema hace necesario para el remitente al enviar un mensaje comercial no solicitado el incluir la información en el mismo de la procedencia de los datos de la cuenta de correo, informando de este modo al interesado de cómo acceder a dichas listas para tener la opción de no autorizar futuros envíos.

Las listas de exclusión de envío de comunicaciones comerciales se conocen como **listas Robinson**[114], cuya finalidad tiene el permitir a los consumidores eliminar su nombre y dirección de los listados de publicidad, con el fin de reducir al mínimo la cantidad de publicidad en forma de mailing dirigido. Por el contrario, aquellos usuarios que deseen la recepción de envíos publicitarios también pueden solicitarlo al servicio de listas Robinson y formar parte de la Lista de Preferencia.

En la actualidad existe únicamente un fichero común de exclusión publicitaria según lo dispuesto en el artículo 45 del **Real Decreto 1720/2007**, aunque no se impide la creación de otros.

[113] Gómez (2010).
[114] Reglamento del fichero de Lista Robinson disponible en https://www.listarobinson.es/reglamento_01.asp

Por el contrario en las listas de inclusión se autoriza el envío de publicidad únicamente a aquellos usuarios que previamente y de forma expresa han manifestado su voluntad de recibirla. Este sistema beneficia potencialmente a los usuarios al respetar sus voluntades de no recibir comunicaciones comerciales no solicitadas ya que no fueron solicitadas previamente, y en caso contrario se vería vulnerado el derecho a la privacidad y provocaría molestias de saturación de los servidores de correo. El problema viene cuando la medida sólo se adopta a nivel nacional, ya que únicamente protegería los envíos dentro del país y no lo haría frente a envíos de otros países con normativa diferente.

Ante esta problemática, mediante este sistema de listas de inclusión opt-in y después de sucesivas Directivas aprobadas que finalmente relegan la actuación a los países afectados, parece que finalmente se puede dar respuesta a las exigencias europeas.

La primera referencia normativa europea sobre comunicaciones comerciales no solicitadas con finalidad comercial la encontramos en la **Directiva 97/7/CE** relativa a la protección de los consumidores en materia de contratos a distancia, a través de medios tradicionales de comercio (no electrónico). En ella encontramos bases comunes como que los envíos promocionales sin petición previa no se admiten, derecho al consumidor de protección de su vida privada, adopción de medidas por parte de los estados miembros para la protección eficaz de los consumidores que no deseen ser contactados, poder conocer el usuario la identidad y finalidad del proveedor, etc. Se puede observar pues, que las comunicaciones comerciales no solicitadas únicamente se pueden realizar a falta de la oposición manifiesta del consumidor, quedando regulado el envío por el sistema opt-out (se permite el envío de publicidad si no hay oposición expresa del destinatario).

Posteriormente, en 1998, la Cámara de Comercio Internacional (CCI) publicó los ***Principios generales sobre la publicidad y marketing en Internet*** en el cual se exige el respeto a los principios de legalidad en el país de origen (veracidad, decencia y honestidad de la publicidad, identificación del anunciante y su publicidad y derechos de los usuarios en materia de privacidad.

En 1999, el Consejo de la Unión Europea aprobó la ***Resolución relativa a la dimensión de los consumidores en la sociedad de la información*** en donde se pone de manifiesto la necesidad de trasladar al entorno electrónico la protección vigente del consumidor en el comercio tradicional y especialmente la adopción de medidas contra prácticas engañosas y desleales en el ámbito de la publicidad así como en las comunicaciones comerciales no solicitadas.

En el año 2000 fue aprobada la **Directiva 2000/31/CE** sobre el comercio electrónico, con el fin de crear un marco jurídico estable que garantice la libre circulación de los servicios de la sociedad de la información así como la libertad de establecimiento entre los estados miembros. Para ello establece el principio de control en origen (el mensaje comercial se somete a la normativa del estado donde se emite tal mensaje. Es contrario al control en destino, que supondrá que el mensaje comercial será sometido a la normativa del estado donde se recibe dicho mensaje) de dichos servicios, comunicaciones comerciales, entre otros, y excluye de su aplicación las comunicaciones comerciales no consentidas. Asimismo se establecen modalidades de protección contra el correo electrónico no solicitado, optando por el sistema de listas de exclusión opt-out dejando abierta la aceptación o no del envío de comunicaciones comerciales no solicitadas. Podemos constatarlo en las consideraciones 30 y 31 de la susodicha Directiva: "*El envío por correo electrónico de comunicaciones comerciales no solicitadas puede no resultar deseable para los consumidores y los prestadores de servicios de la sociedad de la información y trastornar el buen*

funcionamiento de las redes interactivas. La cuestión del consentimiento del destinatario en determinados casos de comunicaciones comerciales no solicitadas no se regula en la presente Directiva sino que ya está regulada, en particular, por las Directivas 97/7/CE y 97/66/CE. En los Estados miembros que autoricen las comunicaciones comerciales por correo electrónico no solicitadas, deberá fomentarse y facilitarse la creación por el sector competente de dispositivos de filtro; además, las comunicaciones comerciales no solicitadas han de ser en todos los casos claramente identificables como tales con el fin de mejorar la transparencia y facilitar el funcionamiento de los dispositivos creados por la industria". *"Los Estados miembros que permiten el envío de comunicación comercial no solicitada por parte de prestadores de servicios establecidos en su territorio por correo electrónico sin consentimiento previo del receptor, deben garantizar que los prestadores de servicios consultan periódicamente las listas de exclusión voluntaria en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y las respeten".*

Y en el artículo 7 de la citada Directiva permite a los estados miembros decidir si prohíbe o no el envío de spam, y en este último caso, los requisitos que el mismo deberá cumplir: la identificación del mensaje como correo no solicitado y el respeto a las listas de exclusión voluntarias.

La Directiva es quizá demasiado genérica y no detalla la información relativa a cómo ha de realizarse este control, no establece plazos en los que obligatoriamente deben consultarse las listas de exclusión, ni simplemente si el sistema partirá de listas públicas o privadas, o sus condiciones.

Entre las excepciones al principio de control en origen declara la licitud de las comunicaciones comerciales no solicitadas, por tanto, queda sometida a la legislación del país en el cual se recibe la comunicación comercial.

Esta directiva, contrariamente a otras legislaciones como la americana, no establece ninguna palabra clave común para todos los estados miembros que deba figurar en el encabezamiento del mensaje y no obliga a que la

identificación de mensaje como no solicitado conste en el espacio destinado al asunto del correo electrónico, además no obliga al remitente a proporcionar una dirección de correo electrónico válida y funcional a la que el destinatario pueda dirigir su deseo de no recibir más correos comerciales y tampoco obliga a incluir en tales mensajes enlaces a las listas de exclusión.

En el ordenamiento jurídico español, se ha incorporado la **Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico** con el fin de generar confianza y seguridad en el entorno de las telecomunicaciones, regulando el régimen jurídico de los servicios de la sociedad de la información y de la contratación en red.

Hasta el año 2002 en Europa había una legislación pendular con normas que compartían el principio opt-in y otras que se inclinaban por los opt-out en mayor cantidad, reconocidas a nivel europeo. Pero es con la llegada de la **Directiva 2002/58/CE** sobre la privacidad y las comunicaciones electrónicas, cuando se hace una apuesta por la postura opt-in que es más restrictiva, modificando pues las Directivas 97/7/CE y 97/66/CE.

Dicha Directiva ha armonizado las condiciones en las que las comunicaciones electrónicas pueden realizarse con fines de venta directa al prohibir su envío si no ha sido autorizado previamente por su destinatario.

Concretamente el artículo 13 de la directiva, relativo a las comunicaciones no solicitadas, ha sido fruto de la cooperación internacional a nivel intraeuropeo en la lucha antispam y de la que forma parte la Agencia Española de Protección de Datos integrando el CNSA (red de contacto de las autoridades responsables en materia spam), responsable de la regulación y el control de las comunicaciones comerciales no solicitadas de la Unión Europea y del Espacio Económico Europeo. Este artículo es el punto en común de los estados miembros y tiene la finalidad de establecer un marco intraeuropeo eficaz en el intercambio de

información en denuncias sobre spam. Además ha unificado en la unión europea la obligatoriedad de obtener el consentimiento previo para el envío de comunicaciones comerciales no solicitadas con independencia del medio utilizado de envío, aunque la directiva no establece el método efectivo para obtener dicho consentimiento, pudiendo obtenerse de varias formas; en concreto, acudiendo a la consideración número 17 de la Directiva, se puede constatar que "*el consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre, inequívoca y fundada de la voluntad del usuario, por ejemplo mediante la selección de una casilla de un sitio web en Internet*". No obstante, tampoco la directiva obliga al remitente a dar una dirección de correo electrónico válida para que el destinatario pueda exigirle a aquel la no inclusión en su lista de destinatarios, ni a proporcionar en el correo publicitario un enlace a las listas de exclusión, así como tampoco queda prohibido el envío de mensajes electrónicos no solicitados por el denominado "consentimiento previo suave"[115].

En el párrafo segundo del artículo 13 de la citada Directiva se establece una excepción al consentimiento previo: "*en el contexto de la venta de un producto o servicio previo el remitente podrá utilizar la dirección de correo sin consentimiento previo siempre y cuando el contenido del envío publicitario esté relacionado son productos o servicios similares a los de la relación contractual y se le facilite siempre el derecho de oposición al tratamiento de sus datos sin cargo alguno y de manera sencilla*".

En este mismo sentido, el artículo 29 de la misma Directiva relativo a la protección de los datos, indica cómo debe ser interpretado el consentimiento previo y sugiere que esta excepción debe ser interpretada restrictivamente tal y como viene recogido en el Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la presente Directiva. Esto implica que los mensajes comerciales sólo podrán ser remitidos a

[115] Plaza (2002)

aquellos que hayan ofrecido sus datos de contacto dentro de la venta de un producto o servicio, lo que requerirá que se tenga en cuenta el periodo de tiempo durante el cual el consentimiento pueda ser considerado como válido y permita el envío de tales mensajes. Únicamente la persona física o jurídica que haya recolectado los datos, tiene la facultad para enviar correos electrónicos comerciales al titular de dichos datos. Esto provoca una limitación al marketing de productos o servicios similares, como se reconoce en dicho artículo.

Retomando el artículo 13 de la citada Directiva, es importante prestar atención a los siguientes párrafos de dicho artículo:

3- En este punto se establece la prohibición para todo envío de correo electrónico o SMS no contemplado en la excepción a una persona física con fines de venta directa, o bien sin el consentimiento previo, o bien respecto de los abonados que no deseen recibir tales comunicaciones (listas de exclusión) y deja en manos de la legislación nacional (desde el momento de la transposición de la Directiva) la elección de entre las dos posibilidades.

4- Se prohibirá, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación, o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones. Pese a la transposición del texto comunitario a la Ley General de Telecomunicaciones, en dicha Ley no se hace mención a la ilicitud de tal ocultamiento, falsificación o inexactitud que sometiera al destinatario a un error en cuanto a la dirección del mensaje o a la identidad de su iniciador, aunque dicha carencia puede quedar salvaguardada por el artículo 20.1 de la LSSICE del que puede desprenderse que "*los prestadores de servicios deberán facilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado*".

5- En este punto se deja en manos de la transposición de la Directiva por parte de los estados miembros extender el régimen de consentimiento previo a las comunicaciones destinadas a las empresas ó personas jurídicas[116].

Finalmente, en el 2002, se aprueba la **Directiva 2002/65/CE** por la que se modifican la Directiva 90/619/CEE del Consejo y las Directivas 97/7/CE y 98/27/CE, que en su artículo 10 amplía el consentimiento previo al prever restricciones a las comunicaciones comerciales no solicitadas como el consentimiento previo en caso de comunicaciones no solicitadas por medio de fax y llamadas automáticas y para técnicas de comunicación individual distintas a las enumeradas no autorizadas sin consentimiento previo o realizadas si no ha habido oposición manifiesta.

Ante el fenómeno del spam, el Derecho regula lo que puede, pero debido a que es un fenómeno a nivel mundial y por el principio de territorialidad en la aplicación de las normas de cada estado, sumado a la inexistencia de una legislación internacional en la materia, hace que sea difícil poder controlar este fenómeno. Esta ausencia de legislación única aplicable al entorno de Internet ha impulsado a las instituciones europeas a legislar y cooperar internacionalmente con el fin de asumir una serie de principios generales sobre el comercio electrónico y la publicidad.

Debido a la debilidad que provoca lo anteriormente comentado, paralelamente se han desarrollado herramientas tecnológicas (mecanismos antispam) para poder combatirlo que pretenden hacer de barrera ante el spam, de forma más o menos acertada, que son empleados por los agentes afectados por tal fenómeno; además se estudiarán los sistemas de

[116] Plaza (2002).

autorregulación que veremos más adelante en este apartado del proyecto, que sentarán una serie de normas a seguir a través de códigos deontológicos y sellos de confianza, para la posible resolución extrajudicial de conflictos ocasionados por la materia de estudio, y una mayor generación de confianza para los afectados por esta problemática, pretendiendo unificar los mecanismos tecnológicos, legales y éticos para lograr en conjunto poder frenar la problemática derivada el spam o las comunicaciones comerciales no solicitadas.

Retomando la legislación, en España, la primera vez que se reguló el fenómeno spam fue en 2002 con la llegada de la LSSICE, que fue criticada por muchos sectores por ser bastante restrictiva en materia de envíos publicitarios no solicitados ya que prohibía el envió de comunicaciones comerciales no solicitadas excepto las consentidas expresamente por el destinatario. La ley era contraria a la normativa de protección de datos y a la propuesta de Directiva sobre la privacidad de las comunicaciones electrónicas ya que no autorizaba el envío de correos a direcciones obtenidas en el curso de anteriores relaciones contractuales ni a las obtenidas de fuentes de acceso público. Los expertos se preguntaron entonces cuanto tiempo pasaría hasta que se modificara la Ley relativa al spam, ya que la Directiva 2002/58/CE sobre la privacidad de las comunicaciones electrónicas aprobada un día después de la ley española, regulaba el envío de comunicaciones electrónicas no solicitadas de manera no idéntica a como la Ley española lo hacía. Un año después, en 2003, la nueva LGT (Ley General de Telecomunicaciones) efectuaba tales modificaciones de la parte dedicada al spam.

La Directiva reguló el envío de spam mediante el principio opt-in, pudiendo únicamente enviarse correos no solicitados a aquellos que lo han

consentido previamente de forma expresa, con lo cual, respecto de la anterior regulación existente, deja de compartir el principio opt-out que permitía el envío de correos electrónicos no solicitados a todos aquellos que previamente no se hayan opuesto a su recepción. Esta evolución es una apuesta clara por los derechos individuales por encima de la libertad de mercado[117].

La regulación en la normativa española en materia de spam antes de su modificación (en 2003 con la LGT) fue elogiada por las asociaciones de usuarios informáticos como la Asociación de Usuarios de Internet (AUI) por suponer un primer paso hacia el control del fenómeno spam, pero a su vez fue muy criticada por asociaciones de empresas que operan en Internet, por no poder competir con el resto de empresas europeas que están sometidas a una regulación del spam menos restrictiva. Pero ya con la llegada de la LGT, se modificó la parte dedicada al spam, flexibilizando los requisitos para el envío de correos no solicitados por parte de las empresas. Tal modificación incluye una excepción a la prohibición del envío de comunicaciones comerciales no solicitadas sin consentimiento previo que no existía en la anterior Ley, en el caso del contexto de una relación contractual previa sobre productos o servicios similares que en un pasado el destinatario adquirió, haciendo posible en este caso a las empresas el envío de correos electrónicos comerciales a destinatarios que adquirieron en el pasado productos o servicios similares al ofertado. Con lo cual, en la nueva LGT se integra al ordenamiento jurídico español lo previsto en el mencionado artículo 13 de la Directiva 58/2002/CE. Aunque hay algo menos de precisión que en la Directiva en cuanto a la generalidad de la expresión “productos o servicios similares” a los que finalmente fueron contratados con el cliente. La

[117] Plaza (2004)

Directiva es más precisa al exigir que la dirección de correo sea obtenida en el contexto de la venta del servicio o producto.

En la práctica en España lo anteriormente comentado se puede observar en el caso de una empresa que manda comunicaciones comerciales no solicitadas sobre un producto/servicio a un cliente del que previamente ha obtenido sus datos de correo electrónico por una vía diferente a la del contexto de un contrato previo existente con el cliente, (aquí la Directiva europea prohibiría esto) pero de forma lícita según la LOPD (por ejemplo se ha obtenido de una guía de profesionales), lo cual sería lícito en España. Según expertos como Plaza Soler[118] que ya ha sido citado previamente, se debería haber mantenido en la legislación española el requisito que mantiene la Directiva europea de que la dirección de correo electrónico sea obtenida durante el procedimiento de contratación con el cliente.

La LSSICE exige autorización previa y expresa, mientras que la Directiva europea únicamente habla de consentimiento previo. Al igual que también hay diferencia entre ellas en la forma de obtención de los datos de contacto, como hemos visto en el anterior párrafo y en otros aspectos que hemos visto previamente en el presente proyecto.

Hay que resaltar, que la adaptación de la Directiva europea para los distintos países que la conforman ha sido dispar en algún aspecto. En el presente proyecto se ha centrado únicamente en el ámbito europeo y español, obviando las particularidades en el ordenamiento jurídico concreto del resto de estados europeos.

Retomando las cuestiones deontológicas relacionadas con el spam, recordamos que la difícil tarea de legislar en Internet es debida a la ausencia de límites de carácter temporal, a la aterritorialidad (opuesta al principio de

[118] Plaza (2004)

territorialidad que acota la aplicabilidad de las legislaciones estatales y define la jurisdicción competente) y a la globalidad que implica la deslocalización de las actuaciones y dificulta los intentos de regulación.

Aunque hay juristas expertos en la materia, como Vázquez Ruano, que consideran que "*Internet no es un espacio sin regulación, sino que la dificultad se halla en el correcto conocimiento acerca de los principios normativos que son de aplicación en cada caso porque el carácter internacional del nuevo medio supone que los actos que en él se lleven a cabo pueden estar sujetos a diversos sistemas jurídicos nacionales al mismo tiempo*"[119].

Ante la dificultad de poder regular normativamente Internet, por los motivos anteriormente expuestos, y con el fin de proporcionar seguridad jurídica a los afectados, una posible solución se encuentra en la **autorregulación** frente al pluralismo legal existente en la Red. La autorregulación se puede definir como la observación de pautas de conducta cuyo cumplimiento se ha fijado previamente como objetivo, es decir, supone que los sometidos al sistema de autorregulación asuman, observen y hagan cumplir las reglas establecidas a tal fin. Este sistema de autorregulación pues contempla la supervisión del cumplimiento efectivo de las normas, auditorías periódicas para comprobar el grado de cumplimiento de las empresas adheridas, creación de sistemas extrajudiciales de resolución de conflictos o la concesión de sellos de confianza que identifican a la empresa como adherida al sistema de autorregulación.

En un sistema autonormativo, el cumplimiento del mismo solo tiene potestad en aquellos que previa y voluntariamente se han comprometido a cumplirlo. Una creación eficaz del mismo supone un elemento básico para limitar el flujo de contenidos no deseados, nocivos e ilícitos. La

[119] Vázquez (2008)

autorregulación implica la consulta y la representación adecuada de las partes implicadas, la creación y el respeto de códigos de conducta, la existencia de organismos nacionales que faciliten la cooperación a escala comunitaria y la evaluación nacional de los marcos de autorregulación.

En un sistema de autorregulación (autonormativo) existen dos mecanismos que conforman este sistema: los **códigos de conducta**[120] o éticos (códigos deontológicos) y los **sellos de confianza**. Por ello para lograr una autorregulación estos códigos de conducta son la base, y se elaboran a partir de pautas de comportamiento que establecen límites jurídicos en el marco electrónico y buscan la adecuada tutela de intereses de las partes intervinientes. Asimismo se establecerá el órgano competente encargado de la supervisión y observación de las pautas y de la resolución de posibles conflictos. Como están sometidos al principio de legalidad, no pueden contener pautas más flexibles o inflexibles que la de los preceptos mínimos que se contiene en la normativa vigente. Para generar confianza y seguridad en el usuario o consumidor de los servicios de la sociedad de la información, éstos han de participar en la elaboración de estos códigos de conducta según van siendo elaborados.

El establecimiento de sellos de confianza constituye "*el mecanismo de identificación y acreditación de la vinculación a normas deontológicas insertadas en las páginas web de los titulares que permite la discriminación positiva a favor de los comprometidos con dichas normas y decisiones de los órganos de resolución extrajudicial de controversias*"[121], es decir, el sello es la manera de identificar la voluntad de aquellas empresas que se han adherido voluntariamente al desempeño de unas prácticas de conducta empresarial que vienen recogidas en el código ético, siendo partidarias de la realización de "buenas prácticas" empresariales.

[120] Los códigos de conducta vienen comprendidos en el artículo 16 de la Directiva 2000/31/CE sobre el comercio electrónico.
[121] Vázquez (2008)

Tal ha sido su importancia que ha sido incentivada en el ámbito del comercio electrónico por organizaciones internacionales y organismos gubernamentales, tanto a nivel comunitario como estatal, a través de la Directiva de comercio electrónico y de la LSSICE. Tal Directiva reconoce que los códigos de conducta a nivel comunitario constituyen un "*instrumento privilegiado para determinar las normas deontológicas aplicables a la comunicación comercial*"[122]. Además la Directiva añade que "*Los Estados miembro fomentaran la elaboración de códigos de conducta a nivel comunitario a través de asociaciones u organizaciones comerciales, profesionales o de consumidores así como la posibilidad de acceder a los códigos de conducta por vía electrónica en las lenguas comunitarias*"[123].

En el caso de la LSSICE, la misma promueve la elaboración de códigos de conducta por considerarlos un instrumento especialmente válido para la adaptación de la normativa legal a las características específicas de cada sector, y además obliga a los prestadores de servicios de la sociedad de la información de "*disponer de los medios que permitan acceder por medios electrónicos de forma permanente, fácil, directa y gratuita a los códigos de conducta"*[124]*.* Asimismo establece que las Administraciones públicas impulsarán la elaboración y aplicación de códigos de conducta voluntarios por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores y avanza las materias sobre las que podrán tratar y que deberán ser consultables por vía electrónica, *"en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los*

[122] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información, en particular del comercio electrónico en el mercado. Consideración número 32.

[123] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información, en particular del comercio electrónico en el mercado. Artículo 16.

[124] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 10. Párrafo g).

procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información"[125].
Asimismo por su sencillez, rapidez y comodidad para los usuarios, se anima a recurrir al arbitraje y procedimientos alternativos de resolución extrajudicial de conflictos con el fin de reducir las disputas ocasionadas en la contratación electrónica o en los demás servicios de la sociedad de la información[126].

En el sector de la publicidad, el mayor beneficio de la autorregulación consiste en promover una ordenación ética y responsable de la actividad publicitaria en beneficio de los consumidores, la industria y el mercado. Su objetivo es contribuir a que la publicidad sea un instrumento útil y que respete los derechos de los consumidores y la lealtad competencial.

En la autorregulación publicitaria española es importante destacar la labor de la **Asociación para el Autocontrol de la Comunicación Comercial**. En el ámbito de la publicidad en Internet se estableció en 1999 el **Código Ético de Publicidad en Internet**, que en 2002 se integra junto al **Código Ético de Protección de Datos Personales en Internet** de la Asociación Española de Comercio Electrónico para dar lugar al **Código Ético de Comercio Electrónico y Publicidad Interactiva**, abarcando este último tanto las comunicaciones comerciales como los aspectos contractuales de las transacciones comerciales de consumidores a través de Internet y otros medios electrónicos, incluyendo asimismo la protección de los datos personales tanto en comunicaciones comerciales como en la contratación electrónica.
El código establece como principio general para su aplicación el país de origen: "*será aplicable a la publicidad y al comercio electrónico realizado a través de medios electrónicos de comunicación a distancia por personas*

[125] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículos 18.1 y 18.3.
[126] Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. Artículo 32.

físicas o jurídicas con establecimiento permanente en España o dirigido de forma específica al mercado español"[127].

La regulación que establece este código para la publicidad se divide en normas generales, especiales y un tercer grupo de normas relacionadas con el control del cumplimiento del código y la resolución judicial de controversias. El mecanismo de resolución de controversias en materia publicitaria cubre su resolución tanto a nivel nacional como comunitario en controversias transfronterizas. El control del cumplimiento del código corresponde a dos órganos extrajudiciales y sus resoluciones son de obligado cumplimiento para las empresas adheridas al código, estos órganos son el Jurado de la Asociación para el Autocontrol de la Comunicación Comercial, encargado de resolver las reclamaciones en materia publicitaria, el otro es la Junta Arbitral Nacional de Consumo, que resuelve las reclamaciones en materia de contratación electrónica que no han sido resueltas por la Asociación Española de Comercio Electrónico.

En este código, en el primer grupo de normas generales se establece que la publicidad en medios electrónicos deberá ser decente, honesta y veraz, cumplirá la identificación de la publicidad y de su anunciante, así como del principio de información general, coste o precio de acceso al mensaje publicitario e identificación clara de ofertas promocionales, obtención de datos personales y respeto de los derechos de propiedad intelectual o industrial y la lealtad a la competencia.

Para el segundo grupo de normas especiales se aplica a las distintas formas publicitarias en línea. Así, la publicidad enviada mediante mensajes de correo electrónico u otros medios de comunicación individual equivalentes (que vendrá identificada como tal) no se admitirá si no ha sido autorizada o solicitada expresamente por el destinatario[128].

[127] Código Ético de Comercio Electrónico y Publicidad Interactiva. Artículo 2.
[128] Código Ético de Comercio Electrónico y Publicidad Interactiva. Artículo 9.

El código apuesta por el consentimiento regulado por el sistema opt-in (listas de inclusión voluntarias), aunque son admisibles cualesquiera que garanticen la prestación del consentimiento.

Señalar finalmente que el código trata la cuestión de la protección de los datos personales, estableciendo que las empresas sujetas a su ámbito de aplicación deben respetar la legislación en materia de protección de datos personales así como respetar la privacidad de los usuarios, asegurar el secreto y la seguridad de los datos personales por medio de la adopción de mecanismos adecuados que contemplen el estado de la tecnología, la naturaleza de los datos y los riesgos a los que están expuestos[129]. Asimismo prohíbe la recopilación de datos personales por medios fraudulentos, desleales o ilícitos. Las empresas adheridas deberán informar a sus titulares en el momento de la recogida de los datos de la procedencia, del origen, de la identidad del responsable del tratamiento, de la finalidad de su obtención y tratamiento así como de los derechos de acceso, rectificación, cancelación y oposición[130]. Asimismo las empresas proveerán a los usuarios de información clara y comprensible sobre la presencia y finalidad de las *cookies*[131] u otros dispositivos o técnicas similares así como de cuándo queda imposibilitado el acceso a un recurso o servicio por ser necesario el envío de e instalación de cookies[132].

En el uso de la autorregulación hay una clara serie de ventajas en cuanto a la regulación del envío de spam, aunque hay autores contrarios al sistema de autorregulación que se basan en la idea de que si las propias entidades empresariales son las que apuestan por la autorregulación, es lógico pensar que estas apuesten más por sus intereses que por los de usuarios y consumidores.

[129] Código Ético de Comercio Electrónico y Publicidad Interactiva. Artículo 20.
[130] Código Ético de Comercio Electrónico y Publicidad Interactiva. Artículo 21.
[131] Cookies: pequeños ficheros de datos enviados por los servidores web a los programas navegadores.
[132] Código Ético de Comercio Electrónico y Publicidad Interactiva. Artículo 24.

6- Guía para el cumplimiento de la legislación española y europea respecto al spam

Este apartado del proyecto ha sido elaborado a partir del proyecto final de carrera[133] de idéntica temática del año anterior, añadiendo información citada encontrada en otros medios y comentarios propios.

Existe un problema a la hora de reducir el envío de spam por medio de la legislación existente únicamente, y es que es insuficiente por sí sola, por lo cual la Comisión Europea elaboró una serie de Comunicaciones[134] sobre el spam o comunicaciones comerciales no solicitadas, que servirán de base para la elaboración de esta guía práctica para el cumplimiento de la legislación española y comunitaria respecto a la materia. Dichos comunicados se centran en el cumplimiento efectivo de la legislación en torno al régimen de consentimiento previo por los estados miembros y autoridades públicas, en autorregulación de la industria, soluciones técnicas, sensibilización de usuarios, cooperación internacional, reprimir el incumplimiento de la normativa, utilizar el recurso de la E-justicia, y en investigación y desarrollo tecnológico que ayude a reducir la problemática derivada del tema de investigación.

La aplicación del régimen de consentimiento previo será prioritaria en todos los estados miembros. Existen relativas a ello tres normas básicas:

1- El envío de mensajes electrónicos con fines comerciales se supedita al consentimiento previo de los abonados[135]. Existe una excepción a tal consentimiento cuando los mensajes de correo, SMS, o MMS son enviados a clientes con relación contractual previa siempre que sean relativos a

[133] Álvarez (2010)

[134] COM (2004) 28 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones comerciales no solicitadas o spam.

[135] Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

productos o servicios similares a los que dio origen a dicha contratación previa. Éste régimen es aplicado a abonados que son personas físicas, aunque los estados europeos pueden extenderlo a personas jurídicas según su criterio.

2- Es ilegal que el remitente de la comunicación disimule u oculte su identidad.

3- Las comunicaciones comerciales electrónicas, deberán incluir una dirección válida y funcional de respuesta a la cual el abonado pueda solicitar el cese del envío de comunicaciones por parte del remitente.

Para hacer cumplir el régimen de consentimiento previo, tendrá que haber un equilibrio en el que se cumplirán tanto las normas legislativas, tanto estatales como comunitarias, la imposición de normas particulares, como las derivadas de la autorregulación. Para evaluar en la práctica el funcionamiento del mismo, y a fin de establecer medidas adecuadas para problemas concretos, será necesaria la obtención de información objetiva y actualizada relativa a las tendencias que va adquiriendo el spam, denuncias de afectados, dificultades de proveedores de servicios de Internet y de correo electrónico. Así se logrará el equilibrio óptimo para todas las partes implicadas.

A continuación se presentan una serie de acciones e iniciativas para poder velar por el cumplimiento efectivo de la legislación española y europea en esta materia y poder hacer un control efectivo de ello.

-ACCIONES DE APLICACIÓN Y DE CUMPLIMIENTO DIRIGIDAS A LOS GOBIERNOS Y AUTORIDADES PÚBLICAS:

Hay que crear mecanismos que garanticen el cumplimiento de la normativa vigente y evaluar la eficacia de los mismos y su seguimiento en el ámbito de recursos y sanciones, mecanismos de denuncia y cooperación internacional:

-**recursos y sanciones:**

Las sanciones administrativas parecen más adecuadas que los recursos judiciales en materia de spam, su coste es menor y son más ágiles en su gestión. Un problema que presenta es la diversa adaptación a la normativa estatal de los dictados europeos, ya que cada gobierno de cada estado impone la sanción que estima pertinente, no teniendo que ser equivalente en otro estado, además de que los gobiernos estatales no tienen por qué designar la misma autoridad pública como responsable de la vigilia del cumplimiento de la normativa. Además la adaptación europea al ordenamiento jurídico nacional al ser distinta en cada caso particular, hará que en cada estado haya diferencia en las autoridades responsables con potestad de actuación en contra de los delitos cometidos, que una misma denuncia en función del país pueda desembocar o no en una investigación o los actores responsables de iniciarla pueden ser distintos en cada caso. Asimismo los mecanismos de denuncia en cada estado serán diferentes, en unos casos el propio consumidor es el encargado de efectuar la denuncia y en otros casos los mecanismos de denuncia están incluidos en la normativa relativa a la autorregulación competente.

Una solución sería la armonización legislativa de los estados miembros en la tipificación de delitos y regulación de los procedimientos jurídicos aplicables, ya que el problema ocasionado por el objeto de estudio es común a todos los estados y se pretende generar la confianza de los consumidores en el entorno electrónico.

-**denuncias:**

Se debe contar con los mecanismos de denuncia adecuados para que haya una aplicación eficaz de la normativa. En este sentido se fomenta el uso de **buzones electrónicos**, también llamados **buzones spam**, a los cuales los destinatarios de spam podrán enviar las denuncias y los mismos correos spam, lo cual proporciona una valiosa información y anima a los afectados a denunciar las infracciones cometidas en esta materia, así como permite poder hacer un seguimiento y medición de la amplitud y alcance del spam, para tener una asimilación más correcta sobre el mismo y poder fijar prioridades en materia de cumplimiento de la normativa.

En el caso de las denuncias transfronterizas, se da el caso de denuncias formuladas por usuarios en un estado miembro, referidas a la recepción de mensajes no solicitados que han sido emitidos en otro estado miembro distinto. Para una correcta atención de este tipo de denuncias, es indispensable la colaboración y el intercambio de información entre las autoridades nacionales implicadas responsables de ello con el fin de evitar el solapamiento de competencias y la duplicidad de funciones entre las distintas autoridades involucradas. A tal efecto la cooperación transfronteriza en la lucha contra el spam fraudulento y engañoso se ampara en el reglamento relativo a la cooperación en materia de protección de los consumidores[136].

-**cooperación internacional:**

Por el carácter transfronterizo del spam, se hace necesaria una sólida cooperación internacional con el fin de hacer extensible el régimen del consentimiento previo aplicable a las comunicaciones comerciales no solicitadas con destino u origen en redes de comunicación ubicadas en la Unión Europea al resto de comunicaciones procedentes de países no comunitarios. Esto es más

[136] COM (2003) 443 final. Reglamento relativo a la cooperación en materia de protección de los consumidores.

complicado de lograr, pero es vital conseguirlo ya que la mayor parte del spam que llega a Europa procede de países no comunitarios, con lo que serán objetivos de la cooperación internacional el promover la aprobación de una legislación adecuada en países extracomunitarios, garantizar la aplicación real de las normas vigentes e impulsar la cooperación con el sector privado, especialmente con proveedores de servicios de Internet y de correo electrónico para poder localizar a los remitentes de spam.

Son ejemplos de ello la participación activa en foros destinados a la lucha antispam promovidos por organismos como la Organización de Cooperación y Desarrollo Económicos[137] (OCDE), la Unión Internacional de Telecomunicaciones[138], las Naciones Unidas[139] o los acuerdos suscritos[140] y los encuentros iberoamericanos[141].

Algunas iniciativas impulsadas por la Comisión Europea en el ámbito de la cooperación internacional han sido:

-Creación de la red de contacto de las autoridades responsables en materia de spam con el fin de favorecer el intercambio de experiencias y mejores prácticas en la lucha contra el spam y facilitar la colaboración para la aplicación transfronteriza de la legislación.

-Plan de acción de Londres, con el fin de establecer un procedimiento de cooperación transfronterizo a nivel mundial por medio de la reagrupación de veinte autoridades de los países encargados del seguimiento de la aplicación de la legislación en la materia.

[137] En 2006 adopta una recomendación sobre la cooperación transfronteriza para dar cumplimiento a legislación sobre el spam en la que instaba a las autoridades responsables a compartir información y colaborar.

[138] Asamblea Mundial de Normalización de las Telecomunicaciones. Resolución 51. Lucha contra el correo basura (spam). Florianópolis, 2004.

[139] Declaración de la Cumbre Mundial sobre la Sociedad e la Información. Ginebra, 2003.

[140] En España destaca el acuerdo de entendimiento del 2005 entre la Agencia Española de Protección de Datos y la Comisión Federal del Comercio estadounidense de ayuda mutua para facilitar el cumplimiento de la legalidad en materia de correo electrónico comercial.

[141] Tercer encuentro Iberoamericano de protección de datos. Cartagena de Indias, 2004.

-Cooperación entre la Unión Europea y EEUU, Canadá, China y Japón, especialmente en el ámbito de la lucha contra los contenidos no deseados, nocivos e ilícitos.

Esto eran iniciativas a nivel europeo, y en este mismo sentido, España y en concreto la Agencia Española de Protección de Datos, ha firmado varios documentos de colaboración y asistencia recíprocas con las instituciones encargadas tanto a nivel comunitario como extracomunitario, con el fin de promover la cooperación internacional. Se pueden observar a continuación:

-**Relaciones con Europa:**

La AEPD forma parte del grupo CNSA compuesto por autoridades nacionales encargadas de la regulación y el control de las comunicaciones comerciales no solicitadas de la UE y del Espacio Económico Europeo. Este grupo ha acordado la creación de un marco intraeuropeo para el intercambio de información sobre denuncias relativas a spam, indicando el modo de proceder ante las mismas.

El punto en común entre los países comunitarios se puede ver en el artículo 13 de la Directiva 2002/58/CE. En virtud de este acuerdo, al recibir una denuncia internacional, previamente al envío a la autoridad nacional competente, ha de verificarse la viabilidad de ésta y comprobar que el denunciante es una persona física. Asimismo se informará al denunciante de que sus datos personales serán cedidos a otra autoridad, manteniendo el secreto de las informaciones y denuncias.

-**Relaciones con Estados Unidos:**

En EEUU hay una normativa en la lucha contra el spam dispar a la europea, concretamente, en EEUU se establece el sistema opt-out de exclusión voluntaria, contrariamente al caso europeo opt-in de inclusión voluntaria, con lo

cual se autoriza el envío de comunicaciones comerciales sin autorización previa del destinatario, mientras éste no manifieste su oposición a recibirlas.

En 2004 la AEPD firmó un convenio de acuerdo de cooperación administrativa para luchar contra el spam con la Comisión Federal del Comercio de EEUU, en el que ambas partes se comprometen a facilitar información de usuarios y empresas relacionadas con el spam, se promueven códigos de conducta que respeten las buenas prácticas, se intercambia información relativa a soluciones técnicas avanzadas en la materia con el fin de estar actualizados en las novedades crecientes, colaboración entre universidades de los respectivos países para promover la investigación, el establecimiento de cursos y conferencias sobre la materia y una asistencia mutua en las investigaciones elaboradas.

-**Relaciones multilaterales:**

Se ha visto ya el ejemplo en el citado Plan de Actuación Conjunta (London Action Plan), cuyo objetivo principal es el desarrollo de contactos internacionales para la investigación en casos de spam. Los suscritos a este plan asumen el impulso de las comunicaciones entre ellos, con el fin de supervisar más eficientemente el cumplimiento de la normativa, organizar conferencias periódicas que tratan la materia o favorecer el diálogo entre organismos públicos e industria para la actuación conjunta y cooperativa.

-**Relaciones con Iberoamérica:**

La AEPD, intentado fijar posiciones comunes sobre la protección de datos personales en los países iberoamericanos, en 2004 participó en el mencionado III Encuentro Iberoamericano, en el que se trataron temas como el ataque a la privacidad en el sector de las comunicaciones electrónicas e Internet y la lucha antispam. Se acordaron medidas técnicas y legislativas para evitar el spam, promover la colaboración internacional o impulsar iniciativas de autorregulación

en el sector de las comunicaciones electrónicas con el fin de poder complementar el ordenamiento legislativo.

-**Foros internacionales:**

La AEPD activamente participa y colabora en los foros de la ITU (Unión Internacional de Telecomunicaciones), que es un organismo de las Naciones Unidas encargado de dirigir la Cumbre Mundial sobre la Sociedad de la Información; en los foros de la OECD Task Force que es el encargado de dar respuesta internacional a las distintas políticas, coordinar la lucha antispam, facilitar la aplicación de leyes fronterizas o promover códigos de buenas prácticas en el sector.

Otro foro, el Foro Abuses[142] es una iniciativa que reúne a alunas organizaciones profesionales privadas que han de trabajar a diario para evitar los impactos y amenazas sobre los sistemas de información. Sus objetivos principales están relacionados con la lucha contra abusos informáticos como el spam, códigos maliciosos, ataques a sistemas informáticos o violaciones de los derechos de la propiedad intelectual. En este foro, las organizaciones participantes intercambian información relevante para combatir los ataques cpn el fin de reducir las amenazas y minimizar su impacto. La cooperación de este foro tiene su equivalente europeo en E-COAT (European Cooperation of Abuse Fighting Teams).

-RECURRIR A LA E-JUSTICIA PARA REFORZAR LA COORDINACIÓN EUROPEA EN LA LUCHA CONTRA EL SPAM:

Uno de los objetivos de la UE es la creación de un espacio de libertad, seguridad y justicia. Con esta idea surge el Espacio Europeo de Justicia (EEJ) con el fin de establecer los instrumentos legislativos necesarios destinados a garantizar el reconocimiento mutuo de las decisiones judiciales y la cooperación

[142] http://www.abuses.es/

entre autoridades judiciales nacionales, mejorando el acceso de los ciudadanos a la justicia a través del portal e-Justicia, y proporcionando eficacia en la acción judicial.

Este portal tiene la finalidad de orientar e informar al ciudadano europeo de los sistemas de redes y procedimientos judiciales, de los instrumentos judiciales etc. para evitar el hecho de que el usuario no pueda defender sus derechos en otros países miembros comunitarios al desconocer el ordenamiento jurídico vigente correspondiente. En definitiva, se proporciona al ciudadano la información tanto nacional como europea de los derechos que éstos tienen y la información necesaria del ordenamiento jurídico correspondiente en casos de denuncias pertenecientes a otros estados de la UE para su defensa sea cual sea la nación comunitaria en la que se inició el hecho ilegítimo en la ley vigente.

Hay una serie de propuestas y recomendaciones dirigidas por expertos a los órganos judiciales y los cuerpos y fuerzas de seguridad de los estados miembros:

-Favorecer y estimular de forma activa la formación continua de jueces y fiscales expertos en la materia.

-Cooperación entre los jueces y los cuerpos y fuerzas de seguridad del estado con el fin del ágil intercambio de información entre ellos.

-Autoridad para poder requerir a los operadores y proveedores de servicios de Internet, la información relativa a las direcciones IP generadoras del hecho ilegítimo cuando haya sospecha fundada e estas actuaciones ilegítimas.

-Disponer de recursos suficientes para detectar a los remitentes de spam activos que ocultan su identidad sirviéndose de la de otros usuarios, como hemos visto que es posible en precedentes capítulos del presente proyecto.

-ACCIONES Y TÉCNICAS DE REGULACIÓN PARA LA INDUSTRIA

La industria, y más en concreto los proveedores de servicios de Internet, debe desempeñar una labor indispensable en la lucha contra el spam, ya que en

el caso de los proveedores de servicio, ellos son el medio por el que fluye el spam.

Ya que la normativa desarrollada en esta materia tiene su razón de ser en el mercado y en la economía, la industria debe tomar un papel decisivo al convertir el régimen de consentimiento previo en una práctica comercial cotidiana.

Esto último se puede dar en el caso de los proveedores de Internet y de correo electrónico, los cuales podrían contribuir a la lucha antispam, si en sus contratos suscritos con los clientes incorporasen en las cláusulas de los mismos la prohibición de no utilizar sus servicios para el envío de spam, y en caso de incumplimiento establecerse las sanciones pertinentes.

Asimismo, la industria debería adoptar una política de filtrado del spam más firme y voluntariosa que proporcionara altruistamente información sobre los filtros antispam así como la implementación de los mismos para la generalización en su uso, y que éste fuera lo más acertado en la medida de lo posible.

Como se ha comentado ya, la industria debe tomar parte fundamental en el ámbito de la autorregulación mediante disposiciones contractuales a las nuevas regulaciones normativas, la elaboración y difusión de códigos de conducta o de buenas prácticas adecuados al régimen de consentimiento previo, fomento de prácticas de comercialización aceptables y la utilización de sellos de confianza para la identificación y garantía de los organismos que comparten la autorregulación responsable y respetan tanto el sistema de consentimiento previo opt-in como una normativa basada en los códigos de buenas prácticas, así como en la proposición de soluciones técnicas para dar soporte a la problemática que se plantea en este contexto.

Es importante resaltar que la solución extrajudicial de conflictos que viene comprendida en el artículo 17 de la Directiva 2000/31/CE sobre el comercio

electrónico[143], puede ser especialmente útil en materia de spam y contribuir en el respeto a la nueva normativa. Para su instauración se exige la cooperación entre las autoridades y la industria.

Las soluciones técnicas parten de la adopción de medidas de seguridad en los servidores y el desarrollo de herramientas de filtrado del spam. Pero como se ha visto en anteriores capítulos del proyecto, no todas las técnicas de filtrado ofrecen las mismas garantías en materia de protección de datos e intimidad, e incluso pueden plantear problemas de eficacia al filtrar correo útil que el filtro considera spam (falsos positivos) conociendo los efectos derivados de ello o al revés en el caso del no filtrado de los correos spam (falsos negativos).

Las recomendaciones para los proveedores de aplicaciones de filtrado de spam, se plasman en programas compatibles con el régimen de consentimiento previo, sensibles a los falsos negativos y falsos positivos, y al reconocimiento de correos electrónicos procedentes de empresas que acogen en sus prácticas los códigos éticos y de conducta y que han obtenido este reconocimiento mediante los sellos de confianza.

Entre otras, las recomendaciones de los expertos dirigidas a los fabricantes y proveedores de servicios son las siguientes:

-Mejorar las actuaciones de los operadores para orientar las medidas de seguridad al bloqueo de determinados servicios como el bloqueo del correo saliente, fácilmente monitorizable a través de un filtro para las máquinas con IP identificadas asociadas a un uso malicioso del servicio de correo, ya sea

[143] Los Estados miembros velarán por que, en caso de desacuerdo entre un prestador de servicios de la sociedad de la información y el destinatario del servicio, su legislación no obstaculice la utilización de los mecanismos de solución extrajudicial, existentes con arreglo a la legislación nacional para la solución de litigios, incluso utilizando vías electrónicas adecuadas; alentarán a los órganos responsables de la solución extrajudicial de litigios, en particular de litigios en materia de productos de consumo, a que actúen de modo tal que proporcionen garantías de procedimiento adecuadas a las partes afectadas; e incitarán a los órganos responsables de la solución extrajudicial de litigios a que informen a la Comisión de las decisiones relevantes que tomen en relación con los servicios de la sociedad de la información, y a que le transmitan todos los demás datos sobre prácticas, usos o costumbres relacionados con el comercio electrónico.

por emisión de spam, malware o troyanos o de aquellas máquinas que alojan sitios fraudulentos en Internet.

-Aplicar políticas avanzadas de gestión de correo electrónico y proporcionar un servicio de salida de correo cortado por defecto, obligando a que el envío de ese correo sea validado previamente por el servidor del proveedor ISP en el cual se puede instaurar un mayor control del flujo de comunicaciones con restricciones y medidas de seguridad contra el mal uso del coreo electrónico.

Asimismo en este sentido, la Comisión Europea insta a las empresas a adaptar las prácticas de venta directa, prácticas contractuales y códigos de buena conducta a la normativa vigente de protección de datos y al régimen de consentimiento previo opt-in. Las recomendaciones de la comisión para los proveedores de servicios son el aplicar una política de filtrado del correo electrónico que se ajuste a las recomendaciones emitidas especialmente por el grupo de trabajo sobre la protección de datos.

-ACCIONES DE SENSIBILIZACIÓN DIRIGIDAS A CONSUMIDORES Y USUARIOS DE LAS REDES DE TELECOMUNICACIONES

En este sentido hay propuestas en el ámbito de la prevención, la educación, el papel que deben adoptar los gobiernos, autoridades públicas, agentes del mercado y asociaciones de consumidores en esta materia. Todo ello se hace llegar al usuario mediante campañas de información dirigidas a los distintos grupos donde se dé a conocer los riesgos en la utilización de las comunicaciones en la Red, el conocimiento de la nueva normativa y los derechos de empresas y consumidores, reflejando las prácticas de comercialización aceptables (ajustadas al régimen de consentimiento previo), el concepto de recogida legítima de datos personales o simplemente proporcionar información y herramientas como sistemas de filtrado para que el usuario pueda hacer uso de las mismas con el fin de reducir el spam, así como una guía para efectuar las

denuncias pertinentes, conocer los mecanismos de solución extrajudicial de conflictos, o conocer las asociaciones de usuarios activas en esta materia.

Los estados de la UE han invertido en campañas de sensibilización dirigidas a los usuarios y consumidores en materia de spam como las anteriormente descritas como el programa **Safer Internet**[144] que a nivel comunitario es concebido para combatir el spam entre otros incidentes de seguridad. Dicho programa se articula en tres ejes principales:

-Implantación de una red europea de líneas directas llamadas *hotlines* que permiten a los ciudadanos denunciar los contenidos ilícitos y nocivos de Internet y que trasladan las denuncias a la instancia pertinente con la intención de reducir el flujo de spam circulante. En este sentido es esencial un sistema de autorregulación adecuado, y a tal fin se crea el foro **Una Internet más segura** con el objetivo de intercambiar experiencias e información en el ámbito de la autorregulación.

-Desarrollo de herramientas de filtrado antispam para limitar el contenido adecuado para menores de edad.

-Iniciativas de sensibilización con el objetivo de informar de cómo proteger a los menores de los contenidos inadecuados para ellos, y de informar sobre los problemas de seguridad relacionados con el uso de Internet, así como de cuestiones relacionadas con la protección del consumidor, la protección de datos personales y la seguridad de la información y de las redes de comunicación.

La continuidad de este programa lo encontramos en el nuevo programa **Safer Internet Plus**[145] que persigue la finalidad de garantizar una cobertura y cooperación de alcance europeo e incrementar la eficacia mediante el intercambio de información, fomentando un uso más seguro de la Red y del resto de tecnologías en línea sobre todo para menores. El nuevo programa

[144] http://europa.eu/legislation_summaries/information_society/internet/l24190_es.htm
[145] http://europa.eu/legislation_summaries/information_society/internet/l24190b_es.htm

busca una inversión en las citadas *hotlines* y en medidas tecnológicas para la gestión de contenidos no apropiados, no deseados o perjudiciales. La inversión en hotlines se plasma en líneas nacionales con capacidad para interactuar y cooperar con otros centros de líneas directas del resto de europa, que recogen datos cualitativos sobre su funcionamiento y que mediante la implantación de un nodo coordinador de la red, permitirá una mayor celeridad en el intercambio formativo de información y aumente la capacidad operativa de las líneas.

Por último es interesante destacar la **Agenda de Túnez**[146], que es adoptada por la Cumbre Mundial de la Sociedad de la Información en el año 2005 y que resalta que la seguridad en Internet es uno de los ámbitos en los que resulta necesario mejorar la cooperación internacional.

-INVESTIGACIÓN Y DESARROLLO TECNOLÓGICO

La UE y la industria, conscientes de la importancia del desarrollo tecnológico y científico aúnan esfuerzos con el fin de crear un Espacio Europeo de Investigación. A tal fin, se impulsaron los programas marco de investigación y desarrollo tecnológico por parte de la Comisión Europea, que constituyen marcos generales de las actividades de la UE en el ámbito de la ciencia, la investigación y la innovación.

Particularmente, el **sexto programa marco**[147], para el periodo comprendido entre el 2002 y el 2006, constituye el principal instrumento legal y financiero de la UE para aplicar el Espacio Europeo de Investigación. Entre sus diversos programas hay proyectos específicos para ayudar a frenar el spam y luchar contra otras formas de programas perniciosos, que centran su investigación, entre otras, en los estudios de tecnologías de la seguridad y confidencialidad de los sistemas informáticos, así como velar por los derechos y la vida privada de los ciudadanos. Las medidas adoptadas en este sentido son la creación de una

[146] http://www.itu.int/wsis/doc2/tunis/off/6rev1.doc (en inglés).
[147] http://europa.eu/legislation_summaries/research_innovation/general_framework/i23012_es.htm

comunidad científica especializada en el control de los programas maliciosos, la puesta a punto de una infraestructura europea que controle el tráfico a través de la Red y la elaboración de filtros adaptables contra el *phising* que permitan detectar amenazas desconocidas y el fraude en Internet.

Por último destacar uno de los programas del **séptimo programa marco** para el periodo del 2007 hasta el 2013, en concreto el **programa de Cooperación** que incluye entre otros, un apartado de "seguridad y el espacio" que da continuidad a la línea de estudio de nuevas medidas para garantizar la seguridad de las redes de información.

Visto todo lo anterior, hay una serie de factores que parecen influir en la eficacia de los mecanismos de aplicación vistos en este apartado:

-La naturaleza y los mecanismos de denuncia y los recursos a disposición de particulares y empresas.

-El conocimiento de los usuarios de sus derechos y modos de actuación en caso de vulneración de los mismos.

-Existen autoridades reguladoras que carecen todavía de poderes coercitivos, y por tanto, ocasiona el problema de la incapacidad de las mismas para tener la potestad de hacer cumplir el ordenamiento legislativo mediante la imposición de sanciones.

-La coordinación y claridad entre las autoridades nacionales competentes, ya que en ocasiones se produce un solapamiento de funciones entre ellas.

-La coordinación y cooperación entre los distintos estados de la Unión Europea y entre éstos y los estados que no pertenecen a la misma.

Para finalizar, además de todas las medidas previstas presentadas a lo largo del presente proyecto para reducir el spam, es interesante prestar atención a una medida extra, sencilla y efectiva que no se ha dado hasta el momento: fijar

una política de cobro aplicada sobre las comunicaciones comerciales, es decir, que el coste económico previamente estipulado de emitir una comunicación a través de la Red, recaiga directamente sobre el emisor de la comunicación comercial, persuadiendo al mismo del envío reiterado y masivo de spam, hecho que además de reducirlo, descolapsaría la red y reduciría en la medida de lo posible la problemática asociada al envío de spam.

7- Conclusiones

Es sabido que Internet hoy en día es un medio de comunicación plural, mundial y estandarizado, que presenta grandes oportunidades para la expansión del comercio y la economía a nivel mundial.

Los beneficios del uso de las Tecnologías de la Información y las Comunicaciones son cuantiosos y considerables tanto para las organizaciones como para los usuarios individuales y la evolución de las TIC en el seno de la Sociedad de la Información ha permitido un avance para todos. Pero lamentablemente este avance ha propiciado un nuevo entorno para la delincuencia y el fraude en Internet, permitiendo una constante evolución en el uso inadecuado e ilegitimo que puede hacerse por medio de las TIC.

Hay que ser conscientes de la magnitud que puede alcanzar, como se ha visto en el presente proyecto, el fenómeno del spam y de todos los problemas asociados que el mismo puede acarrear. Es necesario que exista una concienciación sobre el problema ya que sin ésta, a pesar de las medidas de protección que puedan tomarse, no se logrará una solución ante esta problemática. Además de la sensibilización, asimismo es necesario que haya una formación tanto individual como en las organizaciones sobre ese fenómeno, con un compromiso adecuado de todas las partes afectadas, especialmente por parte de las organizaciones y organismos públicos competentes en esta materia con el fin de adoptar medidas resolutivas como ya hemos visto en otros apartados de este proyecto, sancionando en caso necesario aquellas conductas ilegítimas que se pretenden erradicar en la medida de lo posible.

Se ha intentado buscar un equilibrio en la legislación entre aquellos que defienden el derecho fundamental de la privacidad y son contrarios al spam, y

aquellos que defienden el derecho de la libertad de información y la libertad de empresa, o simplemente aquellos individuos u organizaciones que hacen del uso del spam el medio óptimo para el desempeño de sus actividades comerciales, satisfaciendo las necesidades económicas de un mercado que no quiere renunciar a esta modalidad publicitaria que optimiza sus resultados claramente, ya que si su práctica fuera prohibida en un país, las empresas de este estado estarían en desigualdad de condiciones ante empresas de otros países que si la permitieran.

Las comunicaciones comerciales electrónicas pues, son un importante mecanismo a través del cual fácilmente y de forma económica una organización puede dar a conocer sus productos o servicios y captar clientes en cualquier parte del mundo. El problema es que estas comunicaciones comerciales electrónicas no solicitadas han alcanzado proporciones inquietantes, ocasionando graves problemas, por ello ha ocasionado uno de los retos más importantes a los que se enfrenta Internet y la Sociedad de la Información.

La recepción del spam puede incurrir en sobrecostes para los destinatarios como tiempo en su procesamiento, gastos de almacenamiento, saturación del servicio de coreo y de acceso a internet, y otra serie de problemas en la figura del delito informático (phising, hoax, suplantación de identidad, etc.) que pueden ocasionar graves consecuencias como se ha ido viendo a lo largo del presente proyecto, generando una general desconfianza. Hay gran cantidad de remitentes de spam que emplean procedimientos ilícitos durante la recolección de datos personales de contacto, sin previo consentimiento de los titulares del mismo que además no informan del uso o tratamiento que tendrán tales datos personales, vulnerando los principios normativos que rigen la materia tanto en materia publicitaria como en materia de protección de datos de carácter personal.

Recordemos que la obtención, el almacenamiento y tratamiento de los datos de carácter personal requiere que el titular de los mismos posea la información necesaria y manifieste, de acuerdo con ésta, de modo libre, inequívoco e informado su conformidad. Pero en el supuesto de que la finalidad justifique el tratamiento de la información personal mediante la difusión publicitaria, la LOPD tiene previsto el uso de los datos personales recopilados con fines comerciales de fuentes accesibles al público como resultado de un previo consentimiento del titular, no siendo necesaria tal conformidad en los casos en que se hubiera mantenido una relación comercial o administrativa con la entidad que recaba la información.

Asimismo para mantener la licitud, las comunicaciones comerciales se deben identificar como tales al igual que la identidad de su remitente y deben proporcionar un acceso gratuito y sencillo para la cesación de tales comunicaciones comerciales en el caso que el destinatario así lo desee, aunque hay emisores de spam que se niegan a cumplir la normativa vigente y que ocultan la procedencia de los mensajes publicitarios o no los presentan como tal.

Ya hemos visto que por el principio de aterritorialidad y de la naturaleza internacional de Internet dificulta el cumplimiento normativo, es por ello junto con la excesiva dispersión normativa (LOPD, LSSIC, LGT, Directivas comunitarias, Comunicaciones, o las distintas adaptaciones nacionales en su ordenamiento jurídico de las Directivas europeas) por lo que resulta un complejo entramado jurídico bastante complejo en relación a la materia.

La norma general es que las comunicaciones comerciales emitidas a través de redes electrónicas se adecuen a las normas publicitarias vigentes y de aplicación en el estado desde el que se emiten, debiendo ser aceptadas por los

estados miembros si dichos envíos son lícitos en el país de origen. Si bien esta regla general en el caso de la publicidad comercial no solicitada queda exceptuada al establecerse la posibilidad de que un estado miembro limite e impida dicha publicidad aún en el caso de que el envío sea lícito en el país de origen.

A pesar de ello, el problema sigue pendiente respecto de los envíos publicitarios procedentes de estados que no pertenecen a la Unión Europea o al Espacio Económico Europeo, que no están obligados al cumplimiento de las directivas comunitarias. La solución a ello consiste como ya hemos visto en la autorregulación y la redacción normas de códigos éticos de buenas prácticas y al establecimiento de sellos de confianza para las organizaciones que comparten la autorregulación.

Desde el punto de vista de los aspectos técnicos relacionados con el spam, destaca la incesante transformación a la que se encuentran sometidas las técnicas empleadas por los spammers, por lo que es igualmente necesaria la mejora de las soluciones antispam para que sigan siendo efectivas. A esto se añade la utilización de redes de ordenadores zombies, las llamadas botnets, en las que se incluyen miles de equipos comprometidos y se derivan las responsabilidades del spam enviado. La evolución de los tipos y nuevos medios por los que se envía el spam, a través de telefonía móvil, Voz sobre IP o mensajería instantánea, confirma que las técnicas empleadas por los spammers son cada vez más ingeniosas y sofisticadas, persiguiendo ir un paso por delante y sortear las protecciones antispam.

La problemática del spam ha hecho surgir el debate sobre qué correos electrónicos pueden considerarse spam y cuáles no. Aunque las listas de distribución y el propio spam tienen en común el envío de un volumen grande

de correos, existen dos mecanismos básicos para el control y diferenciación de estos envíos: la opción de aceptación, o sistema opt-in, previa a la primera comunicación, y la opción de cancelación u opt-out en cada comunicación. Estos sistemas, que ya están regulados normativamente, exigen el consentimiento del usuario de modo explícito, incluso mediante una doble confirmación, además de ofrecer la opción de cancelación de los correos que el usuario está recibiendo. Fuera de esta validación, todo correo masivo se entiende como spam.

En este sentido, los expertos señalan el desajuste entre países con sus correspondientes marcos jurídicos que dificultan la focalización nítida del problema. La simple diferencia entre los sistemas opt-in u opt-out según la parte del mundo de que se trate puede abrir brechas en un problema que no conoce fronteras. Teniendo en cuenta las propias características de la Red, globalidad y universalidad, además de la autorregulación, es necesario la consecución de acuerdos o tratados multilaterales (nacionales e internacionales), puesto que los mayores problemas que se plantean en la lucha contra el spam radican en el origen del mismo. En la mayoría de las ocasiones el spam recibido procede de fuera de nuestro país y, en consecuencia, extralimita nuestro marco jurídico y escapa a su persecución y sanción. Aunque ya se han visto las formas de poder atajar este problema en anteriores apartados de este proyecto.

Dentro del marco legal del spam, los expertos juristas reafirman y destacan la encomiable labor del cuerpo jurídico español en defensa de los ciudadanos y organizaciones ante un problema tan complejo, que se desarrolla en un contexto no menos complejo como el de Internet como piedra basal de la Sociedad de la Información.

En cuanto al impacto social del spam, las cifras indican que este tipo de incidencia es más frecuente que otros, como el phishing o incluso el malware. Los usuarios colocan a la publicidad como el mayor problema de Internet, tanto la que se emite en ventanas emergentes (pop-ups) como la recibida en el correo spam. La mayor consecuencia es que el spam ha generado una desconfianza relativa entre los usuarios habituales del correo electrónico; sin embargo no ha podido constatarse una reducción de su uso.

Los expertos ponen el acento en la necesidad, entre otras, de la inclusión de la definición de correo electrónico, así como de la matización de conceptos como el de “envío masivo de comunicaciones comerciales" del artículo 38 de la LSSICE, que en ocasiones puede derivar en una interpretación desacertada. En cuanto a las comunicaciones comerciales por correo electrónico, ya se han indicado las ventajas que podría suponer incluir ciertas modificaciones en estas comunicaciones para dar una mayor transparencia al envío y confianza a los destinatarios.

El fenómeno de spam subsistirá frente a cualquier sofisticada solución tecnológica mientras las prácticas de usuarios y organizaciones no sean reconducidas hacia un uso adecuado de las tecnologías de la información y, en concreto, el empleo responsable del correo electrónico.

Las opiniones de los expertos en la materia en cuanto a las actuaciones que conviene tener presentes en la protección global frente al spam se centran en los siguientes puntos:

-La motivación hacia la formación de usuarios y organizaciones prevalece como mejor herramienta para prevenir el spam.

-La adecuada gestión de seguridad de los sistemas de información, con el establecimiento de una política de seguridad que determine sin ambigüedades responsabilidades, mecanismos, condiciones y clasificaciones necesarias para el acceso, almacenamiento, transmisión y eliminación de la información manejada en las organizaciones.

-El diseño y aplicación de políticas de uso del correo electrónico en toda la estructura de las organizaciones.

-La aplicación de sencillas medidas preventivas ante hábitos inadecuados (como la publicación directa de direcciones de correo electrónico en las páginas web corporativas)

-El establecimiento de protecciones proactivas (listas grises, marco de trabajo, etc.) en los servidores de correo, en combinación con salvaguardas reactivas en ellos y en los propios clientes de correo.

Estos expertos en seguridad, destacan asimismo un conjunto de aspectos particulares que deberían sumarse a los anteriores con el fin de conseguir soluciones globales y robustas frente al spam. En este sentido, destacan:

-Impulso decidido hacia la calidad y efectividad en los sistemas, mediante certificaciones o evaluaciones de productos o servicios antispam.

-Demanda de esfuerzo en la consolidación tecnológica, desarrollando herramientas y mecanismos más potentes que permitan mayor control.

De otro lado, los responsables de empresas de marketing electrónico ponen el acento en la relevancia e impacto del spam en el desarrollo de su actividad empresarial. Dado que el ejercicio de su modelo de negocio requiere del envío lícito de correos masivos, este debe quedar bien diferenciado del spam, para poder llegar a sus clientes soslayando las medidas antispam establecidas por las

estafetas de correo que les dan servicio. En esta línea, los expertos señalan como fundamentales las siguientes líneas de actuación:

-Establecer acuerdos con las grandes empresas que ofrecen servicios de correo electrónico y con proveedores de servicios de Internet para que permitan el envío de estos correos, basados en la elaboración de listas blancas.

-Compromiso frente a las posibles quejas o reclamaciones de usuarios.

-Esfuerzos en la divulgación de su modelo de negocio y de los aspectos legales que diferencian el correo propio del marketing electrónico del spam. En tanto que el marco jurídico español vela por el derecho de estas empresas a realizar su actividad comercial, las mismas trabajan por el refuerzo y cumplimiento de la legislación en lo referido a sus intereses.

Las conclusiones de los expertos procedentes de distintos sectores señalan la labor fundamental en la mitigación del spam que deben desarrollar las administraciones públicas: iniciativas de concienciación, formación, evaluación, protección, coordinación y organización de los diferentes agentes que se enfrentan a este problema.

8- Bibliografía

- AEPD (2005). "Guía para la lucha del Spam". AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. Disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N-SPAM--ap-V.-30-mayo-cp-.pdf

- AIMC (2010). "Navegantes en la Red. 12ª encuesta AIMC a usuarios de Internet". Asociación para la Investigación de Medios de Comunicación. Disponible en http://www.inteco.es/studyCategory/Seguridad/Observatorio/Estudios_e_Informes/Biblioteca/AIMC_navegantes

- Álvarez Vizcaíno, Manuel (2010). "Estudio de los aspectos legales y éticos del Spam". Licenciatura en Documentación. Universidad Politécnica de Valencia. Disponible en http://riunet.upv.es/bitstream/handle/10251/9107/DOEEFC87_09.pdf

- Aparicio Vaquero, Juan Carlos (2005). "Régimen jurídico de las comunicaciones comerciales realizadas a través del correo electrónico". En "La Ley: revista jurídica española de doctrina, jurisprudencia y bibliografía", número 4, 2005, pp. 1476-1489. Disponible en http://dialnet.unirioja.es/servlet/revista?codigo=846

- BIT DEFENDER (2010). "Informe sobre las amenazas cibernéticas en el segundo semestre de 2009". BIT DEFENDER. Disponible en http://www.inteco.es/studyCategory/Seguridad/Observatorio/Estudios_e_Informes/Biblioteca/Informe_bitdefender_amenazas_2S2009

- COIT (2004). "Correo electrónico y SPAM" . COLEGIO OFICIAL DE INGENIEROS DE TELECOMUNICACIÓN . Madrid. Disponible en http://es.scribd.com/doc/19049881/Spam#outer_page_19

- Dabendofer, Thomas P (2005). "Impact Analysis of spam". Swiss Federal Institute of Technology. Zurich. Suiza.

- FUNDACION TELEFONICA (2009). "La Sociedad de la Información en España 2009". FUNDACION TELEFONICA. Madrid. Disponible en http://sociedadinformacion.fundacion.telefonica.com/DYC/SHI/InformesSI/

- Gómez-Juárez, Isidro (2010). "Consideraciones sobre el régimen jurídico del "spam" con ocasión del nuevo artículo 29.2 de la Ley de Competencia Desleal". En "Datos personales.org: la revista de la Agencia de Proteccion de Datos de la Comunidad de Madrid", número 46. Disponible en http://dialnet.unirioja.es/servlet/revista?codigo=2880

- INE (2007). "*Encuesta Anual de Coste Laboral, año 2006"*. Instituto Nacional de Estadística. Publicada el 5 de septiembre de 2007. Disponible en http://www.ine.es/jaxi/menu.do?type=pcaxis&path=%2Ft22/p132&file=inebase&L=0

- INTECO (2007). "Amenazas silenciosas en la Red: rootkits y botnets". INTECO. Disponible en http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Notas_y_Articulos/Amenazas_silenciosas_en_la_Red_rootkits_y_botne_11

- INTECO (2007). "Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing". INTECO. Disponible en http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_sobre_usuarios_y_profesionales_de_enti_137

- INTECO (2008). "Estudio sobre la situación, naturaleza e impacto económico y social del correo electrónico no deseado 'spam'". Instituto Nacional de Tecnologías de la Comunicación. Disponible en http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Estudio_spam

- INTECO (2009). "Estudio sobre la seguridad de la información y la e-confianza de los hogares españoles: 1er trimestre de 2009". Instituto Nacional de Tecnologías de la Comunicación. Disponible en http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/Informe_1T_2009

- McAfee (2011). “Informe de McAfee sobre amenazas: Cuarto trimestre de 2010”. McAfee Labs. Disponible en http://www.inteco.es/studyCategory/Seguridad/Observatorio/Estudios_e_Informes/Biblioteca/informe_amenazas_McAfee

- ONTSI (2010). ”La sociedad en Red 2009 Informe anual. Edicion 2010”. Observatorio Nacional de las Telecomunicaciones y de la SI. Disponible en http://www.ontsi.red.es/informes-anuales/articles/id/4814/informe-anual-2009-edicion-2010.html

- Panda Security (2011). “Informe anual PandaLabs 2010”. Panda Security. Disponible en http://www.inteco.es/studyCategory/Seguridad/Observatorio/Estudios_e_Informes/Biblioteca/informe_anual_PANDA

- Plaza Soler, Juan Carlos (2002). “La regulación de los correos electrónicos comerciales no solicitados en el derecho español, europeo y estadounidense”. En “Revista del poder judicial”, número 68. Disponible en http://dialnet.unirioja.es/servlet/revista?codigo=1214

- Plaza Soler, Juan Carlos (2004). “Los correos comerciales no solicitados un año después de la LSSICE”. En “Revista de la contratación electrónica”, número 45, pp. 3-37. Disponible en http://dialnet.unirioja.es/servlet/revista?codigo=2973

- Sanz de las Heras, Jesús. (2003) “Evaluación de alternativas para reducir el spam”. RedIRIS http://www.rediris.es/mail/abuso/doc/MedidasAntiSPam.pdf

- SPAMINA (2008). “Libro Blanco del Spam”. SPAMINA. Disponible en http://download.spamina.com/marketing/Libro_Blanco_Spam_2008.pdf

- Vázquez Ruano, Trinidad (2008). “La protección de los destinatarios de las comunicaciones comerciales electrónicas”. Editorial Marcial Pons. Madrid.

LEYES, DIRECTIVAS, COMUNICACIONES

- Ley 26/1984, de 19 de julio de 1984, General de Defensa de los Consumidores y Usuarios.

-Ley 34/1988, de 11 de noviembre de 1988, General de Publicidad.

-Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

- Ley 7/1996, de 15 de enero de 1996, de Ordenación del Comercio Minorista.

- Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos.

-Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y Comercio Electrónico. (Ley de Comercio Electrónico o LSSICE).

-Ley 32/2003, de 3 de noviembre de 2003, General de Telecomunicaciones.

- Real Decreto 1332/1994, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de carácter personal.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia.

- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

-Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información, en particular del comercio electrónico en el mercado. (Directiva sobre Comercio Electrónico).

- Directiva 2002/19/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso).

- Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización).

- Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva Marco).

- Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).

-Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

- Directiva 2002/65/CE del Parlamento Europeo y del Consejo, de 23 de septiembre de 2002, relativa a la comercialización a distancia de servicios financieros destinados a los consumidores.

-Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

-COM (2000) 890 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos, 2000.

-COM (2001) 298 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Seguridad de las redes y de la información: propuesta para un enfoque europeo, 2001.

-COM (2003) 65 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las Comunicaciones electrónicas: el camino hacia la economía del conocimiento, 2003.

-COM (2003) 443 final. Propuesta de reglamento del Parlamento Europeo y del Consejo relativo a la cooperación en materia de protección de los consumidores, 2003.

-COM (2004) 28 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones comerciales no solicitadas o spam, 2004.

-COM (2006) 251 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una estrategia para una sociedad de la información segura diálogo, asociación y potenciación, 2006.

-COM (2006) 334 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la Revisión del marco regulador de la UE de las redes y los servicios de comunicaciones electrónicas, 2006.

-COM (2006) 688 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la lucha contra el spam, los programas espía y los programas maliciosos, 2006.

-COM (2007) 267 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Hacia una política general de la lucha contra la ciberdelincuencia, 2007.

-COM (2009) 140 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Informe sobre el mercado único europeo de las comunicaciones electrónicas en 2008.

-COM (2010) 253 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Informe sobre el mercado único europeo de las comunicaciones electrónicas en 2009.

-Documento del grupo de trabajo sobre protección de datos del artículo 29: Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea, adoptado el 21 de noviembre de 2000.

- Carta de los Derechos Fundamentales de la Unión Europea.

- Reglamento del fichero de Lista Robinson. Disponible en https://www.listarobinson.es/reglamento_01.asp