ESTUDIO DE LOS ASPECTOS LEGALES Y ÉTICOS DEL SPAM

Proyecto Fin de Carrera

Licenciatura en Documentación

Autor: Manuel Álvarez Vizcaíno

Director: Juan Vicente Oltra Gutiérrez

Universidad Politécnica de Valencia

Valencia, Septiembre 2010

El envío masivo de mensajes electrónicos no solicitados constituye un fenómeno preocupante. El spam, en efecto, representa entre el 50% y el 80% de los mensajes enviados a usuarios finales. La mayor parte de los mensajes no solicitados procede de países terceros (Asia y Estados Unidos, principalmente) si bien el 25% de ellos es difundido por los países europeos.

Se ha calculado que el coste del spam a nivel mundial alcanza los 39.000 millones de euros[1].

[1] Lucha contra el spam, los programas espía y los programas maliciosos.

Índice

Objetivos

En el presente trabajo se aborda la problemática del spam desde sus aspectos legales y éticos. A tal fin es enunciada y comparada la normativa comunitaria y la estatal española aplicable, así como los sistemas de autorregulación y la solución extrajudicial de conflictos, con alguna referencia al sistema normativo norteamericano.

Se describen las características del medio por el que el spam fluye masivamente, a saber, las redes de información y comunicación así como el cambio experimentado por la publicidad, razón de ser del spam, cuyas normas publicitarias de carácter general también se aplican a la actividad publicitaria electrónica.

Se abordan, asimismo, las comunicaciones comerciales electrónicas, consentidas o no, por ser ésta la expresión empleada por la normativa comunitaria para referirse a un sector emergente de capital importancia para la Sociedad de la Información y las economías europeas. No obstante, pese a que las no consentidas fueron concebidas para referirse al spam, su definición elude la característica más importante del spam: su carácter masivo y reiterado que sólo estará contemplado, en el caso español, en el régimen sancionador.

También se aborda la vulneración plural de derechos de usuarios y consumidores por el envío de spam tales como la intimidad, los datos de carácter personal, la competencia desleal, la publicidad engañosa, el ataque a sistemas y redes de información o la ciberdelincuencia.

Finalmente se elabora una guía para el cumplimiento efectivo de la normativa existente cuya finalidad es, si no erradicar la práctica del spam, al menos sí frenarla.

Introducción

En sus inicios la Red Internet fue un medio eficaz de comunicación para posteriormente erigirse en inestimable fuente de información. La tercera etapa de su desarrollo viene marcada por el comercio electrónico y un cambio en la tradicional concepción del ejercicio publicitario que convierte a éste en nuevo mercado para el sector de las comunicaciones electrónicas[2].

Internet no sólo puede ser entendido, como así lo han hecho y aprovechado extraordinariamente las empresas con finalidad comercial o publicitaria, como una red de comunicación de fácil y eficiente difusión. 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.

Su incorporación a la vida económica y social ofrece innumerables ventajas. Todo el mundo reconoce su impacto en la productividad de las empresas y en el nivel de la competitividad de un país. Es una realidad para el 95% de empresas en España como también lo es el correo electrónico que se ha convertido en herramienta indispensable usada por un 94,7% de las empresas de más de 10 empleados.

El correo electrónico constituye una modalidad de comercialización directa de productos y servicios por medio del envío individualizado de mensajes con contenido publicitario.

Su definición según la Directiva 2002/58/CE[3] sobre la privacidad y las comunicaciones electrónicas es *todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse*

[2] Vázquez Ruano, T. La protección de los destinatarios de las comunicaciones comerciales electrónicas, 2008.

[3] a*rt.2)h*

en la red o en el equipo terminal del receptor hasta que éste acceda al mismo. En otras palabras, abarca cualquier mensaje enviado por medio de redes electrónicas que no requiera la participación simultánea del emisor y receptor.

Los servicios abarcados actualmente por la definición de correo electrónico incluyen el correo clásico basado en el protocolo SMTP (*Simple Mail Transport Protocol*), el servicio de mensajes cortos SMS, los servicios de mensajes multimedia MMS, los mensajes en contestadores, los sistemas de mensajería vocal incluidos en los servicios móviles y las comunicaciones enviadas por Internet dirigidas directamente a una dirección IP.

Tal ha sido el éxito del correo electrónico que ha llegado incluso a pervertirse su uso dando lugar a la más común y molesta plaga electrónica, el llamado spam o correo basura y que en la actualidad se extiende a la telefonía móvil.

Las empresas que se anuncian por Internet han aumentando considerablemente. Actualmente podemos decir que la mayoría de empresas dispone de página web desde donde publicita sus servicios y productos y que tiene en el correo electrónico el medio más socorrido para el envío de comunicaciones comerciales. Asimismo, las empresas orientan su política de marketing hacia el aprovechamiento y la 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 finalidad comercial es notable.

El informe[4] que recoge los resultados del observatorio de marketing directo e interactivo realizado entre anunciantes por encargo de la Asociación de Agencias de Marketing Directo e Interactivo para 2009 apunta que el 78,4% de las 213 empresas encuestadas realizan actividades de marketing directo e interactivo.

[4] http://www.agemdi.org/emailing/2009/docs/Observ_MDI09.pdf

Entre los formatos interactivos más utilizados está el e-mailing y el medio interactivo más utilizado es Internet. El uso de aplicaciones y tecnologías web en el entorno Internet se ha visto incrementado significativamente en los últimos años tal y como muestran los diferentes estudios e informes que han ido realizando los distintos grupos e instituciones relacionados con los medios y las tecnologías de la comunicación. Entre los usos de Internet destaca la comunicación con el correo electrónico a la cabeza como más frecuente, según datos del informe anual de la sociedad de la información en España elaborado por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información[5]. Aumenta también la disponibilidad del correo entre particulares que alcanza al 77,4% entre quienes han usado Internet en alguna ocasión, porcentaje que asciende hasta el 90,8% si nos referimos a quienes accedieron la última semana.

El envío y recepción de correos electrónicos también se perfila como uno de los usos más habituales entre la población internauta europea. El 85% de los internautas de la Unión Europea del *grupo de los 27* han hecho uso de la red para enviar y recibir correo. El porcentaje llega al 86% si nos centramos en el grupo de la Unión Europea *de los 15* siendo los holandeses líderes con un 95%. En **España** más del **80%** de los internautas utiliza la Red para el correo electrónico y la búsqueda de información sobre clientes y servicios.

Así, según la 11ª encuesta de la Asociación para la Investigación de Medios de Comunicación[6] para el año 2009 un 71,1% de los 36.000 internautas encuestados usan el correo electrónico varias veces al día. El 35,2% tiene dos cuentas de correo electrónico, el 25,1% tiene tres y el 17,3% una. Entre éstos,

[5] La sociedad en Red 2008: informe anual, 2009.

[6] AIMC. Navegantes en la Red: 11ª encuesta a usuarios de Internet, 2009.

el 69,8%, lo hace a través de una aplicación web mientras que el 28,1% a través de una aplicación de software.

De ese mismo año, los datos arrojados por el informe[7] de la **Fundación Telefónica** muestran que el estilo de vida digital avanza a nivel general entre la población. Tal y como muestra la evolución del grado de digitalización de actividades en España, el 93,7% de la población internauta envía correos electrónicos. A pesar del surgimiento irreversible de nuevas tecnologías a las que ha de hacer frente tales como la mensajería instantánea o las redes sociales, el correo electrónico continúa siendo la herramienta más utilizada por los encuestados con un 56,6% entre los 16 y 24 años y un 43,2% entre los 25 y 34 años. Además el correo electrónico continúa siendo para los usuarios el servicio de Internet más utilizado por delante de la World Wide Web, la transferencia de ficheros FTP, el intercambio de archivos P2P o los chats y foros de discusión con un uso del 96,4%. Asimismo la consulta al correo electrónico desde terminales móviles es el servicio de Internet más usado con un 16% frente al 14%, 11%, 9% y 8% que utiliza el móvil para navegar, buscar información, leer prensa en línea y enviar mensajes, respectivamente.

[7] La Sociedad de la Información en España 2009: 10 años de Sociedad de la información. Fundación Telefónica, 2009.

La publicidad en Internet

La novedad de Internet ha supuesto también que la publicidad haya crecido a la par que ésta y hoy sea un mercado muy relevante. Consecuentemente la publicidad de productos y servicios se ha convertido en elemento fundamental del comercio de nuestros días y constituye un factor relevante para la actividad empresarial.

La publicidad entendida como "*toda forma de comunicación realizada por una persona física o jurídica, pública o privada, en el ejercicio de una actividad comercial, industrial, artesanal o profesional, con el fin de promover de forma directa o indirecta la contratación de bienes muebles o inmuebles, servicios, derechos y obligaciones*[8]*"* tiene su equivalente en la comunicación comercial electrónica entendida como "*toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes y servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional*[9]*"*. Por tanto y, según Vázquez Ruano,[10] "no tendrán la consideración de publicidad las comunicaciones cuya finalidad no sea la promoción directa o indirecta de la contratación de bienes y servicios a cambio de una remuneración ni aquellas que se realicen por cumplimiento de una obligación legal o reglamentaria y no por el ejercicio del derecho a la libertad de información y a la libertad de mercado".

[8] Ley 34/1988, de 11 de noviembre de 1988, General de Publicidad. art.2

[9] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico. Anexo.

[10] Vázquez Ruano, T. La protección de los destinatarios de las comunicaciones comerciales electrónicas, 2008.

El contenido informativo de la publicidad la aproxima al derecho a la información, entendida la publicidad como una de las manifestaciones del derecho a comunicar y recibir información veraz. En opinión de Romero Jaime[11] el interés y difusión públicos, que según la doctrina del Tribunal Constitucional son elementos constitutivos del derecho a comunicar y recibir información veraz, concurren en la comunicación publicitaria porque se trata de información que el ciudadano demanda o que una vez facilitada resulta de su interés y porque su difusión pública resulta inherente a la información publicitaria.

Por otro lado y desde su dimensión creativa, la publicidad se adentra en el ámbito constitucional por el derecho a la producción y creación artística y la libertad de expresión ya que a través de la publicidad se pueden difundir pensamientos, opiniones e ideas, tal y como expone la Ley publicitaria[12]: "*es ilícita la publicidad que atente contra la dignidad de la persona o vulnere los valores y derechos reconocidos en la Constitución, especialmente en lo que se refiere a la infancia, la juventud y la mujer".*

No es ésta, sin embargo, la posición del los tribunales Supremo y Constitucional al sentenciar "*el fin mismo que caracteriza a la actividad publicitaria marca una diferencia profunda con el derecho a comunicar libremente información veraz por cualquier medio de comunicación, ya que aquélla, aún siendo también una forma de comunicación, se vincula al ejercicio de una actividad comercial, industrial, artesanal o profesional con el fin de promover de forma directa o indirecta la contratación de bienes muebles o inmuebles, servicios… La publicidad, por tanto, no es una manifestación del derecho fundamental a la libertad de expresión, por cuanto este derecho da cobertura a la libre y veraz transmisión de hechos que*

[11] Romero Jaime, Diego Jesús. Del charlatán al spam: publicidad molesta y libertad informática. Tutela judicial del consumidor y acciones de cesación, 2008.

[12] art.3 de la Ley 34/1988 General de Publicidad.

puede permitir a los ciudadanos formar sus convicciones ponderando opiniones diversas e incluso contrapuestas y participar así en la relación de asuntos públicos…, concluye, *es el fin último de la publicidad lo que margina, en definitiva, a esta actividad del ámbito de protección del referido derecho fundamental".*

En cambio tanto la Comisión Europea de Derechos Humanos como el Tribunal Europeo de Derechos Humanos se muestran a favor de la inclusión de la publicidad comercial en el artículo 10 del Convenio Europeo de Derechos Humanos: "*toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencias de autoridades públicas y sin consideración de fronteras".*

De idéntica adscripción es la opinión de Vázquez Ruano[13] para quien *respecto de la demarcación del concepto de comunicación comercial, el ejercicio de la actividad promocional se halla amparado por la protección general reconocida en la Constitución respecto de la libertad de empresa y del derecho a la libertad de información a través de cualquier medio de difusión*.

Pese a la falta de acuerdo a la hora de situarlo al lado de uno u otro derecho constitucional lo cierto es que la publicidad tiene mala prensa y es bastante común afirmar que, entre otros perjuicios, supone un grado de molestia y perturbación en el consumidor destinatario a quien se pretende mover hacia la contratación del bien o servicio objeto del mensaje publicitario. Sin embargo y, a tenor de la labor de los legisladores, parece que la molestia afecta más a las empresas competidoras que a los consumidores al hacerse de ella un juicio de competencia desleal.

[13] Vázquez Ruano, Trinidad. La protección de los destinatarios de las comunicaciones comerciales electrónicas, 2008.

La razón por la que se justifica en la publicidad molesta la infracción es en lo que puede influir en la libre decisión del consumidor a la hora de inclinarse por el producto publicitado y no por otro. Es decir, cuando influye en la posibilidad de que pueda conocer con más sosiego otras ofertas. En otras palabras, la publicidad molesta no es más que una patología de la comunicación publicitaria que tiene lugar cuando el influjo publicitario excede los límites admisibles al punto de condicionar al consumidor la libre determinación en orden a contratar un servicio o producto e impidiendo o dificultando notablemente la posibilidad de acceder a una información contrastada.

Efectivamente, su práctica es ilícita en virtud de las normas existentes sobre publicidad engañosa y prácticas comerciales desleales. La Directiva 2005/29 sobre las prácticas comerciales desleales[14] prohíbe las prácticas engañosas[15] y agresivas[16] así como la venta forzada adoptadas por las empresas en sus relaciones con los consumidores. Se entiende que son aquellas prácticas de la mercadotecnia que tratan de influir indebidamente en el consumidor en el momento de la compra o no de un producto o servicio y relacionadas directamente con la libre elección.

[14] http://europa.eu/legislation_summaries/consumers/consumer_information/l32011_es.htm [consultado el 28/06/2010]

[15] art.6.1 de la Directiva 2005/29/CE sobre las prácticas comerciales desleales: se considera engañosa toda práctica comercial que contenga información falsa o induzca a error al consumidor ay que le haga tomar una decisión sobre una transacción que de otro modo no hubiera tomado.

[16] art. 8 de de la Directiva 2005/29/CE: se considera agresiva toda práctica comercial que merme mediante el acoso, la coacción o la influencia indebida, la libertad de elección del consumidor con respecto al producto y le haga tomar una decisión sobre su compra que de otro modo no hubiera tomado.

De este modo la directiva define los criterios generales que determinan si una práctica comercial es desleal[17] y, así, señalar un conjunto de prácticas de mala fe[18] prohibidas en la totalidad del Espacio Económico Europeo.

Por otro lado, el creciente desarrollo de Internet y, particularmente su aspecto comercial, fundamental para empresarios y consumidores, ha supuesto la aparición de nuevas formas de realizar publicidad por parte de quienes ofrecen bienes y servicios a través de ella. Se trata de un medio óptimo para conseguir objetivos publicitarios de forma rápida y económica.

Internet constituye un medio novedoso como soporte para el desarrollo de campañas publicitarias que permite a los destinatarios de éstas interactuar de diversas maneras. En poco tiempo se ha convertido no sólo en fuente inagotable de información sino también en vehículo a través del cual se facilitan las relaciones comerciales entre empresas y consumidores. Tanto es así que el desarrollo del comercio electrónico ha favorecido la aparición de la publicidad en línea que presenta como ventajas la ampliación del número de personas expuestas a sus mensajes y el incremento sustancial de su efectividad, el desarrollo de nuevos formatos de difusión, la interactividad, la comunicación directa y bidireccional, la actualización en tiempo real, la inmediatez del mensaje, los envíos múltiples, la posibilidad de individualizar al destinatario del mensaje[19], etc.

Éste último es quizá el elemento más destacado de la publicidad: hacer llegar su mensaje de la manera más directa, eficaz e individualizada posible. Tanto es así

[17] art.5.2 de la Directiva 2005/29/CE: una práctica comercial será desleal si es contraria a los requisitos de la diligencia profesional y distorsiona o puede distorsionar de manera sustancial el comportamiento económico del consumidor medio al que afecta o al que se dirige la práctica.

[18] Anexo I de la Directiva 2005/29/CE

[19] Rivero González, D. Régimen jurídico de la publicidad en Internet y las comunicaciones comerciales no solicitadas por correo electrónico, 2003.

que en la medida en que se pueda conseguir delimitar con claridad y precisión a los receptores del mensaje se habrá cumplido su objetivo.

No obstante, la publicidad dirigida por este nuevo medio electrónico, las llamadas telefónicas, el envío mediante fax o correo electrónico de mensajes publicitarios pueden vulnerar derechos civiles ya contemplados en los corpus legales. Ejemplo de esto es la intromisión ilegítima en el ámbito privado por medio del uso ilícito de un dato de carácter personal como es la dirección electrónica de correo al emitir comunicaciones comerciales individualizadas. O la posibilidad de infringir un principio publicitario como es la obligación identificar como tal el mensaje publicitario e incurrir en delito como es la publicidad engañosa y encubierta.

La relevancia de la publicidad comercial de cara a la financiación de los llamados servicios de la sociedad de la información determina la presencia casi constante de las comunicaciones comerciales en la red. Tan significativa presencia obedece además a las características propias del medio: la bidireccionalidad e interacción en la comunicación, la universalidad de la red a la que pueden acceder millones de personas o el bajo coste en comparación con la publicidad de corte tradicional son factores que favorecen la consecución de los objetivos publicitarios.

Dentro de las comunicaciones comerciales en red existen tipos de publicidad que difieren unas de otras en función de cómo se recibe, bien indirectamente a través de la red, bien directamente a través de una cuenta de correo electrónico u otros medios de comunicación electrónica equivalentes.

Son varios los instrumentos o mecanismos de envío de publicidad en línea disponibles: las páginas web que constituyen para los comerciantes y empresas el soporte más frecuente donde anunciar sus servicios y productos, los *banners* o anuncios situados en las páginas web más visitadas, los anuncios intersticiales o de transición entre dos páginas web, los anuncios emergentes o *pop-ups* que se

abren cuando el usuario carga una página web, los *layers* o figuras animadas que al pinchar sobre ellos conducen a la página web del anunciante, las *cookies* o chivatos que sirven para localizar y rastrear los movimientos de un usuario por la red y vulnerar, por tanto, su derecho a la intimidad o la publicidad difundida en grupos de noticias, foros y chats que puede plantear problemas de intrusión o publicidad encubierta y de captación de los datos de los participantes en los foros para el envío posterior no consentido de publicidad a sus cuentas de correo electrónico.

Como decíamos, la publicidad vía Internet es más barata que la enviada a través del correo postal y su difusión se ve ampliamente favorecida. Asimismo permite establecer una comunicación a tiempo real, individualizar servicios y establecer perfiles de consumidores que atiendan a uno o varios criterios aunque sean variables a lo largo del tiempo.

A pesar de la gran cantidad de modalidades publicitarias surgidas desde la aparición de Internet, las comunicaciones comerciales no solicitadas, por su crecimiento y las graves consecuencias que tienen para la protección de la privacidad de los usuarios, parece ser el problema más acuciante en el mercado.

Así pues, el llamado marketing interactivo, posible gracias al avance y desarrollo de las tecnologías de la información y la comunicación, ha sido pervertido por la codicia del mercado y las empresas hasta el punto de emplear técnicas consideradas ilícitas para la captación de datos de carácter personal.

En el caso español el derecho fundamental al que se refiere el artículo 18.1 de la Constitución[20] *garantiza*, según la doctrina del Tribunal Constitucional, *a la persona un poder de control y disposición de sus datos personales integrado por*

[20] *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos.

Viene a configurar un nuevo derecho, el de libertad informática, definido como el derecho a que se requiera el previo consentimiento para la recogida y uso de datos personales, el derecho a saber y ser informado sobre el destino y uso de estos datos y el derecho a acceder, rectificar y cancelar dichos datos.

La polémica surge cuando en el derecho de libertad informática interfieren las prácticas publicitarias inadmisibles o molestas porque, con fines publicitarios, se conservan para posteriores usos de envíos de publicidad comercial los datos personales obtenidos con ocasión de la contratación. O incluso se recaban datos personales sin consentimiento ni conocimiento previo del titular de los datos y se trasmiten de igual modo a terceros violando de este modo el derecho a ser informado tanto de la cesión como del destino.

Así pues, ante la problemática que presenta este tipo de publicidad directa y sus posibles consecuencias para, entre otros, los titulares de datos personales, no es de extrañar que haya sido objeto de interés preferente en los textos legislativos tanto a nivel nacional como comunitario.

La sociedad de la información y el sector de las comunicaciones electrónicas

Hasta hace relativamente poco se hablaba de servicios y redes de telecomunicaciones. En su lugar, actualmente se emplea comunicaciones electrónicas para referirse en una única expresión al conjunto de servicios y redes que operan en la llamada Sociedad de la Información, en adelante SI, y que tienen como finalidad el transporte de señales por medio de cables, ondas, medios ópticos, u otros medios electromagnéticos: red fija, inalámbrica, de televisión por cable y satélite.

¿Qué es, por tanto, la SI? Es un estadio tecnológico de la sociedad merced al cual sus miembros pueden crear, consultar, utilizar y compartir información y conocimientos para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de un desarrollo sostenible y en la mejora de la calidad de vida[21]. Asimismo son servicios de la sociedad de la información[22] "todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario".

La SI es fruto de la gran expansión alcanzada por las redes de telecomunicaciones que, unidas en la ubicua Internet, permiten la creación de un Espacio Europeo de la Información con un mercado interior abierto y competitivo y da lugar a uno de los principales retos de la Unión Europea, cuyas instituciones, califican el conocimiento y la innovación como los motores del crecimiento sostenible indispensables para la construcción de una sociedad de la

[21] González de la Garza, Luís M. Sociedad de la información en Europa, 2008.

[22] Son servicios de la sociedad de la sociedad de la información entre otros y siempre que representen una actividad económica el envío de comunicaciones electrónicas. Fuente: LSSICE. Anexo. Definiciones

información absolutamente integradora, basada en la generalización de las Tecnologías de la Información y el Conocimiento, en adelante, TIC.

La evolución de las TIC ha repercutido en distintos ámbitos de la vida económica, política, jurídica y social. Constituyen el crecimiento de la productividad y de la competitividad del conjunto de la economía europea e influye en el crecimiento y la creación de empleo, la competitividad, la mayor calidad de vida para los ciudadanos de la Unión Europea, la financiación de los servicios de la SI y el desarrollo de nuevos. Su difusión, cada vez mayor, crea nuevas modalidades de comunicación e interacción entre los ciudadanos, las empresas y los poderes públicos al abrir paso a estructuras sociales y económicas novedosas. Concretamente la banca a través de Internet (*e-banking*), el gobierno electrónico (*e-goverment*), el comercio electrónico (*e-commerce*), las relaciones con la administración (*e-administration*), entre otras. Son, las comunicaciones electrónicas, el pilar básico del conjunto de la economía dentro de un marco regulador que impulsa el fomento de la competencia, la consolidación del mercado interior de las comunicaciones electrónicas y el beneficio de usuarios y consumidores.

Tal es el uso que la sociedad hace de las redes de telecomunicación y los sistemas de información, demostrado por la multiplicación de las conexiones a Internet, que la seguridad ha llegado a constituir una verdadera preocupación hasta el punto de afirmar que podemos esperar que el número de actividades ilegales aumente en la medida que lo hace el uso de ordenadores y redes.

En este sentido, la comunicación[23] sobre la revisión del marco regulador de las comunicaciones electrónicas, la creación de una agencia europea encargada de la

[23] COM(2006) 334 final "Revisión del marco regulador de la UE de las redes y los servicios de comunicaciones electrónicas".

seguridad de las redes y la información (ENISA) o el séptimo Programa Marco de Investigación constituyen medidas que la Unión Europea despliega para poder garantizar a los usuarios de las redes y sistemas de información el mayor grado de seguridad.

Así las cosas, la revisión del marco regulador de las comunicaciones propone reforzar las normas en materia de seguridad y de protección de la vida privada con el fin de aumentar la confianza de las empresas y los particulares en el uso de este tipo de comunicaciones.

A tal fin la Comisión propone una serie de medidas entre las que destacan la obligación de los proveedores de servicios de Internet y de correo electrónico específicos a notificar las vulneraciones de materia de seguridad y a mantener informados a sus abonados y la modernización de las disposiciones sobre integridad de las redes.

La agencia ENISA asume el asesoramiento en materia de seguridad a redes y sistemas de información. Su objetivo principal, por tanto, es reforzar la prevención, la reacción y la gestión de los problemas de la Unión Europea vinculados con la seguridad de las redes y la información[24]. Tiene, pues, un papel importante que desempeñar en la lucha contra los delitos informáticos y los ataques contra los sistemas informáticos. Asimismo la creación de un sistema europeo de intercambio de información y de alerta válido para responder eficazmente a las actividades que suponen una amenaza para las redes electrónicas constituye otra de las medidas que la Comisión propone y que eleva a la agencia para el estudio de su viabilidad.

[24]Agencia Europea de Seguridad de las Redes y la Información (ENISA). En http://europa.eu/legislation_summaries/information_society/l24153_es.htm [consultada el 1/07/2010]

Como vemos, para la Unión Europea, el sector de las comunicaciones es uno de los puntales del Espacio Económico Europeo y el grado de seguridad jurídica una condición indispensable[25]. Fomentar la inversión en investigación y desarrollo así como en la prestación de servicios de banda ancha, de redes de tercera generación o la interoperabilidad entre distintas tecnologías conseguirá crear las condiciones adecuadas para alentar las inversiones, la innovación y el desarrollo del mercado tal y como lo demuestra su evolución y la reglamentación en este sector recogidos en los dos últimos informes sobre el mercado único europeo de las comunicaciones electrónicas. Los ingresos procedentes de las telecomunicaciones representaron el 52% del total del sector de las TIC en el año 2008[26]. En el 2009 la crisis económica obligó a los usuarios a gastar menos y según el observatorio europeo de la tecnología de la información el crecimiento fue próximo a cero[27].

Algunas de las iniciativas europeas relacionadas con la SI y el sector de las comunicaciones son:

- la iniciativa e-Europe "una SI para todos" constituye la pretensión de conectar a los ciudadanos europeos en todos los aspectos de su vida, permitiéndoles participar de todas las posibilidades que ofrecen las tecnologías digitales. Tal uso propiciaría una nueva economía basada en el conocimiento. El plan de acción e-Europe 2002 pretende una Internet más rápida, barata y segura, una inversión en las personas y en su formación y el fomento del uso de Internet.

[25] COM(2003) 65 final "Comunicaciones electrónicas: el camino hacia una economía del conocimiento".

[26] COM(2009) 140 final "Informe sobre el mercado único europeo de las comunicaciones electrónicas 2008"

[27] COM(2010) 253 final "Informe sobre el mercado único europeo de las comunicaciones electrónicas 2009"

- la estrategia i2010[28] constituye el marco de la Comisión Europea por el que se determinan las políticas generales de la SI y de los medios de comunicación. Tiene por objeto impulsar el conocimiento y la innovación a fin de mejorar el crecimiento y el empleo en el sector de las comunicaciones electrónicas, la convergencia digital (de tecnologías, redes de comunicación, medios de comunicación, contenidos, servicios) y los desafíos vinculados a la SI.

  Tres son las prioridades para hacer realidad esta integración: la creación de un espacio único europeo de información que promueva un mercado interior abierto y competitivo construido en base a la superación de los retos planteados por la convergencia digital (velocidad, riqueza de contenidos, interoperabilidad y seguridad), el refuerzo de la innovación y la inversión en investigación sobre TIC y el logro de una sociedad europea de la información basada en el acceso universal (sin exclusión de ningún sector de la sociedad), la calidad de vida y la mejora de los de los servicios públicos por medio del fomento de la administración electrónica[29].

El crecimiento del uso de tecnologías asociadas a las redes e Internet ha experimentado un notable aumento y una rápida evolución. Un incremento paralelo a éste lo ha tenido el desarrollo de técnicas ilícitas que han encontrado en la web un medio idóneo de difusión y expansión hasta el punto que han configurado una tipología de delincuencia nueva llamada *ciberdelincuencia* que

[28] i2010: la sociedad de la información y los medios de comunicación al servicio del crecimiento y el empleo. Disponible en: http://europa.eu/legislation_summaries/information_society/c11328_es.htm. [consultado el 07/08/2010]

[29] Plan de acción sobre administración electrónica i2010-07-08. Disponible en: http://europa.eu/legislation_summaries/information_society/l24226j_es.htm. [consultado el 08/07/2010]

ha requerido para su persecución la aprobación de nuevas leyes o la modificación de las ya existentes.

Las administraciones públicas son conscientes de que la SI supone un entorno de grandes beneficios para alcanzar niveles más elevados de desarrollo pero también de riesgos potenciales por lo que éstas deben mejorar su eficacia, su productividad y la calidad de sus servicios sirviéndose de las TIC para lograrlo. Sin embargo, sólo es posible ofrecer tales servicios públicos en un entorno que transmita seguridad y confianza en el ciudadano tal y como recoge la Declaración de Ginebra de 2004 en los principios para construir la SI: "*el fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autentificación, la privacidad y la protección de los consumidores es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC".*

Es en este nuevo contexto donde la protección de los datos personales, la autentificación o la gestión de identidades son cuestiones básicas en las que ningún servicio público o privado puede fallar.

Las instituciones públicas y privadas deben garantizar siempre la seguridad de las transacciones y comunicaciones electrónicas. Los ciudadanos deben tener siempre la posibilidad de controlar el acceso a sus datos personales y las formas de almacenamiento y utilización de dichos datos tal y como establecen las distintas disposiciones normativas sobre protección de datos de carácter personal.

La confianza es, por tanto, clave para el éxito de la nueva SI. Una confianza relacionada con las experiencias de los usuarios y con el deber de respetar su intimidad y a la que se llega a través de garantizar la seguridad en las redes y servicios de comunicación electrónicas.

En este sentido, tanto la Unión Europea como la Cumbre Mundial sobre la Sociedad de la Información, han tomado seriamente la percepción de la confianza con que los usuarios, las empresas y las administraciones acometen el uso de las redes. Una confianza de los ciudadanos respecto a Internet, a los servicios de la Sociedad de la Información y del comercio electrónico, está amenazada por la proliferación de técnicas fraudulentas que tienen en el engaño su razón de ser. Además está relacionada con el deber de respetar la intimidad de los usuarios de las redes. Una intimidad que se percibe fuertemente vulnerada con el envío, entre otros, de comunicaciones no solicitadas con fines comerciales. Amenazas tales como el spam (es posible que un mensaje de correo no solicitado sea también portador de programas espía o maliciosos), los programas espía y maliciosos sitúan a la SI en un contexto de inseguridad y desconfianza.

Ejemplo destacado es la utilización de mensajes de *phishing* que inducen a los usuarios finales a facilitar datos a través de páginas web que imitan las de empresas auténticas y consiguen falsificar identidades y socavar la reputación de empresas.

Los ataques de *phishing* usan la ingeniería social, basada en el engaño, para adquirir fraudulentamente información personal referida principalmente a servicios financieros y para alcanzar al mayor número posible de víctimas utilizan el spam para difundirse. Una vez que llega al correo del destinatario intenta engañar a éste para que faciliten datos de carácter personal, normalmente conduciéndolos a sitios web falsificados de bancos persuadiéndolo para que introduzca datos de la cuenta bancaria, contraseñas, etc.

Tratándose de un fenómeno basado en el engaño el usuario ha de asumir cierta responsabilidad y mantener un comportamiento prudente para la utilización segura de la Red. No sólo se ha de hacer uso de herramientas y aplicaciones

específicas como los *firewall* y los cortafuegos complementados con el empleo de medidas básicas como antivirus, antispam, para lograr una navegación segura, sino que a fin de conseguir una protección global, los sistemas operativos y programas se han de mantener actualizados[30].

El envío de spam, favorecido ampliamente por las tecnologías antes citadas, hace que éste pueda llegar a ser abusivo y agresivo además de incómodo y molesto cuando no ha sido solicitado. El destinatario final puede ver cómo en la mayoría de casos y, en ausencia de su expreso consentimiento, su derecho a la intimidad y la privacidad de datos personales son continuamente violados.

El spam es uno de los retos principales de Internet y los legisladores. Se hace necesario un marco jurídico eficaz que prohíba y penalice estas prácticas de difusión comercial masiva que tiene por finalidad la comunicación no deseada y la difusión de nuestros datos personales con finalidad comercial. En la mayoría de casos los datos de se obtienen sin el consentimiento del titular de los datos de carácter personal por medio de técnicas fraudulentas que tienen como finalidad la sustracción de direcciones de correo electrónico procedentes de listas de distribución, foros de discusión, etc.

Serán necesarias, por tanto, distintas actuaciones encaminadas a la aplicación eficaz de las normas y ampliar la cooperación internacional dado que es un problema extraterritorial cuya solución requerirá además la intervención y colaboración de la industria y los consumidores y sus asociaciones representantes.

[30] Vázquez, Ruano, T. La protección de los destinatarios de las comunicaciones comerciales electrónicas, 2008.

El problema del spam

Se denomina *spam* o "correo basura" a todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo la Agencia Española de Protección de Datos, en adelante AEPD, 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*[31].

Se puede decir que esta definición carece de uno de los rasgos más característicos del spam como es su carácter masivo, es decir, su envío personalizado a múltiples destinatarios, rasgo que sí es reflejado, en las definiciones dadas en sus diferentes comunicaciones la Comisión de la Unión Europea:

"Las comunicaciones comerciales no consentidas que se envían masivamente por correo electrónico reciben en el contexto de ***Internet*** *el nombre de spam o correo basura. El spam puede ser definido como el envío masivo e indiscriminado de comunicaciones comerciales o publicitarias no solicitadas por medio del correo electrónico. Estos mensajes no solicitados son a menudo de tipo comercial. El spam es el equivalente electrónico a la invasión en los buzones de nuestros hogares de publicidad impresa no solicitada"*[32].

La palabra spam tiene su origen en la década de los años 60 con un *sketch* del grupo británico humorista *Monty Python* basado en la repetición del término

---

[31] Guía para la lucha contra el spam. Agencia española de protección de datos.

[32] Lucha contra el spam, los programas espía y los programas maliciosos http://europa.eu/legislation_summaries/information_society/l24189a_es.htm#KEY [Consultado el 22/06/2010]

SPAM, abreviatura de *Spiced Ham*, cerdo en lata especiado comercializado por la empresa norteamericana *Hormel Foods*. En dicho sketch el término SPAM se repetía una y otra vez entre todos los platos ofrecidos por la camarera pese a que el cliente no quería tomar SPAM pero no tenía más remedio que tragar con él. Por extensión, spam viene a significar algo carente de valor estético y nutritivo. De ahí que spam, en minúscula para diferenciarla del producto alimenticio sea utilizada, en el ámbito publicitario e informático, para referirse al correo basura, es decir, cualquier mensaje no solicitado, masivo e indiscriminado que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Estos correos se suelen denominar en los países anglosajones *junk mail* o *bulk mail*[33].

La mencionada AEPD recoge en su *Guía para la lucha contra el spam* las diferentes formas del spam o correo basura: correo electrónico (más usado por los *spammers*), ventanas emergentes o *pop ups* (mensajes que aparecen al conectarte a Internet), *hoax* (mensaje de contenido falso y engañoso cuya finalidad es la intercepción de direcciones de correo, saturar los servidores de correo y la red) y el *scam* (no tiene carácter comercial pero sí implicación con el fraude telemático).

Así, en función de su contenido, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) a través del Observatorio de la Seguridad de la Información proporciona la siguiente clasificación[34]:

- 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

[33] Plaza Soler, J.C. La regulación de los correos electrónicos comerciales no solicitados en el derecho español, europeo y estadounidense, 2002

[34] Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing. INTECO, 2007

inferior al de mercado. En algunos casos tiene relación con algunos tipos delictivos, ya que en la actualidad se ofertan por este método productos que infringen la normativa sobre propiedad intelectual, patentes o sanidad.

- bulo o *hoax* es un mensaje electrónico con contenido falso o engañoso, generalmente enviados en cadena y que solicita al destinatario reenvíos posteriores. En ellos se cuenta una historia más o menos verosímil relacionada con injusticias, abusos, problemas sociales, etc. con objeto de captar direcciones de correo electrónico.
- spam con fines fraudulentos: el spam puede ser en muchos casos puente para la comisión de fraudes. La mayor parte de modalidades fraudulentas llegan a sus destinatarios a través de su correo electrónico.
- spam con fines delictivos: a medio camino entre el *hoax* y el fraude a través de un ataque de *spamming* se puede tratar de dañar la reputación de una persona física o jurídica. De modo que este envío masivo suele ser utilizado para propagar rumores sin contrastar su autenticidad.

Aunque se asocia habitualmente al correo electrónico personal también puede afectar a foros, blogs y grupos de noticias. La mayoría de las entidades que emplean esta práctica utilizan EEUU y los países asiáticos para realizar los envíos masivos a todas las zonas del planeta.

El spam sigue siendo el ataque más frecuente con una tasa del 84% de los e-mails en el primer trimestre de 2008 en España. Con un número tan elevado de ataques que ocasionan principalmente pérdidas económicas, desconfianza entre los usuarios y la eliminación de correo legítimo la sofisticación ha evolucionado hacia nuevas modalidades de spam cada vez más difíciles de detectar por los filtros anti-spam.

De modo que tenemos los picos de spam cuya finalidad es el ataque masivo durante un corto periodo de tiempo a una entidad concreta con el objetivo de saturar sus sistemas anti-spam, el spam con adjuntos en tipos de archivos como *PDF, MP3*, el spam de créditos que aprovecha la crisis económica para el envío publicitario fraudulento, el spam apoyado en buscadores, el spam desde cuentas de Gmail capaces de sortear sistemas de seguridad basados en la verificación de un texto empleado para dificultar la captación de direcciones de correo electrónico o spam de contenido más agresivo para captar la atención del destinatario y evitar así que borre el mensaje una vez detectado que es no deseado.

La práctica del spam no es novedosa. También se realiza a través de medios convencionales que son titularidad de una determinada persona como es el correo postal. La diferencia es que su ejercicio en el entorno telemático hace que sea difícil su elusión, genera nuevos riesgos a la intimidad y a la protección de datos de carácter personal, costes económicos o el incremento de actuaciones contrarias a Derecho como los delitos informáticos o ciberdelicuencia.

Hoy día resulta habitual que los usuarios de correo electrónico reciban una importante cantidad de mensajes no solicitados, en muchos casos, inútiles e incluso perjudiciales.

No se puede considerar que las redes de comunicación y, en particular Internet, constituyan un foco de nuevos delitos. Muchas veces son foco de nuevas versiones de prácticas ilegales ya existentes. Si el fraude a través de Internet evoluciona constantemente también lo hacen los usuarios gracias a mejores hábitos de utilización de la Red y a una mayor protección de los equipos.

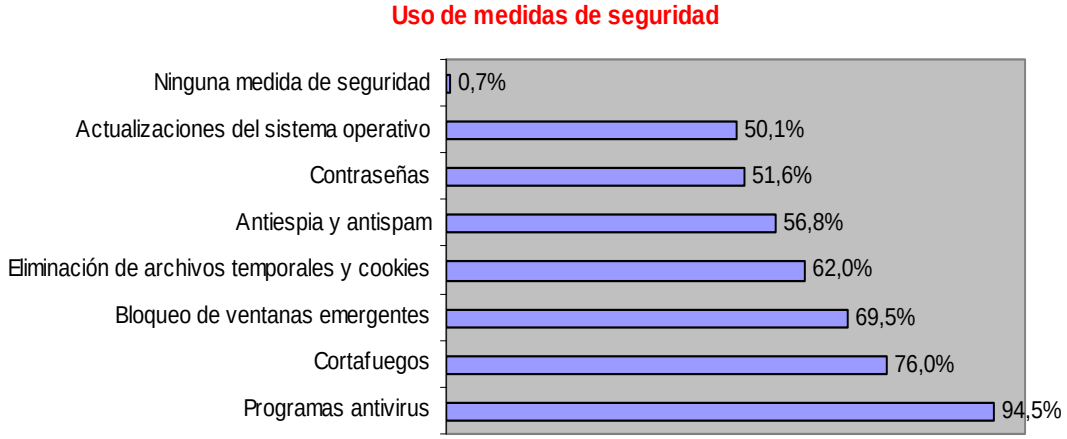
La instalación de programas antivirus en los hogares españoles es prácticamente universal con un 94,5% de los usuarios frecuentes de Internet. En segundo

lugar, la medida de seguridad más utilizada son los programas cortafuego (76%) seguido del bloqueo de ventanas emergentes (69,5%), la eliminación de archivos temporales y *cookies* (62%) y los programas antispam y antiespía (56,8%)[35].

Por lo general los usuarios se decantan por medidas de seguridad automatizables que no suelen requerir del usuario una atención específica. Permiten configurar la automatización de las actualizaciones de las medidas cada vez que el usuario se conecta a Internet de modo que puedes conocer el estado de las mismas, la última actualización, configuración de descarga e instalación y aplicación de avisos y estado.

Los expertos recomiendan como medida de gran interés y relevante en la lucha contra el fraude en Internet la obligatoria implantación de medidas de seguridad en el software por parte de proveedores y fabricantes.

[35] Fuente: Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing. INTECO, 2007



El spam por la propia naturaleza de Internet y la evolución tecnológica de los medios a través de los cuales se distribuye y produce es un problema internacional frente al que hay que actuar cooperativamente. Ha alcanzado proporciones inquietantes. Aunque las estadísticas varían se considera, según fuentes de la industria, que alrededor del 70% del tráfico mundial de correos electrónicos recibidos en 2005 es spam[36].

Varios factores se suman al preocupante problema del spam.

- su crecimiento: el 88,7% del correo mundial en el segundo trimestre de 2009 es spam (casi 9 de cada 10 correos)[37].
- su penetración: entre las causas que más inseguridad provocan respecto del uso de las TIC, se sitúa en segundo lugar por detrás de la incidencia de virus informáticos. También su diversidad que va del spam fraudulento y engañoso al de contenidos ilícitos o perturbadores. Asimismo suponen, en muchos casos, instrumento para la comisión de fraude electrónico (*phishing*[38]*, scam*[39]*,* etc.).

Su espectacular crecimiento tiene varias razones. Por un lado, la disponibilidad más amplia de mejores redes de comunicación y el creciente número de conexiones a Internet suponen para los *spammers* un elevado número de destinatarios potenciales. Por otro, la expansión de las redes de ordenadores

[36] Agencia Española de Protección de Datos. 2005

[37] La sociedad de la información en España 2009. Fundación Telefónica, 2009

[38] Estafa consistente en el envío masivo de correos electrónicos que fingen proceder de bancos u otras entidades con el fin de obtener contraseñas y datos personales de los usuarios para hacerse pasar por ellos en operaciones en línea.

[39] Correo no deseado que implica fraude por medios telemáticos bien vía teléfono móvil o correo electrónico.

llamadas *botnets*[40] ha contribuido a su crecimiento ya que gran parte del spam actual es enviado por estas redes.

Es responsable del conflicto de intereses entre dos colectivos: se enfrenta el derecho de los empresarios a la difusión de su publicidad por medios electrónicos, al igual que lo hacían por los medios tradicionales, con el derecho de los destinatarios a no recibir una publicidad que, favorecida por las tecnologías, llega de forma más numerosa y frecuente.

En la actualidad, los virus (59,6%) y el spam (46,2%), son los dos problemas de seguridad, recordemos aspecto clave de la SI, que más afectan a los internautas.

Ante el elevado número de incidencias relacionados con problemas de seguridad frente a virus informáticos, software malicioso, programas espía o correo no deseado el informe de la Fundación Telefónica ***La sociedad de la información en España 2008*** sitúa, entre las causas, la falta de concienciación de los internautas que se traduce en un uso bajo de medidas de precaución contra el riesgo tal y como muestra el ***Estudio sobre seguridad de la información y la e-confianza de los hogares españoles*** elaborado por Instituto Nacional de Tecnologías de la Comunicación para el año 2007. Según el mismo, la recepción de spam se sitúa entre las incidencias de seguridad que más afecta a los usuarios por delante de códigos maliciosos, las instrucciones remotas en el ordenador, en el correo electrónico, la obtención ilícita de datos personales, etc. Sin embargo el 56,5% de los usuarios afirma no tomar ninguna medida frente al correo no deseado. En el primer trimestre del 2009 los internautas que recibieron

[40] Estos sistemas infectados se conocen bajo el nombre de *botnets* y son utilizados por los emisores de spam para el envío masivo mediante la instalación de aplicaciones ocultas que convierten a estos sistemas en servidores de correo sin que lo sepan sus usuarios. Se calcula que más del 50% de spam se envía desde estos *botnets.*

correos no deseados fueron el 46,2% mientras que un 30,2% usaba filtros anti-spam según datos de la Fundación Telefónica[41].

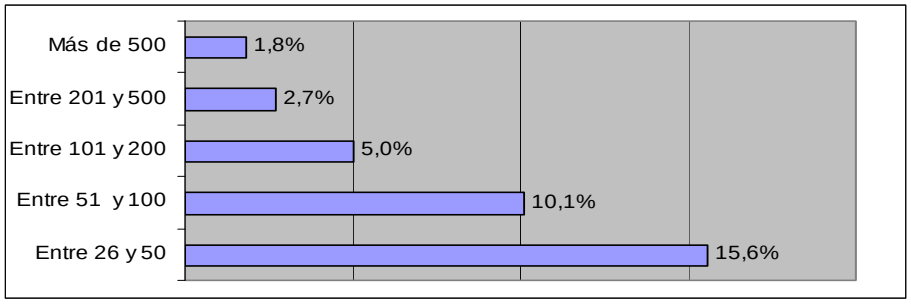
No obstante, las estadísticas mejoran en este sentido con el estudio realizado por la Asociación para la Investigación de Medios de Comunicación[42] (AIMC) en 2009. Según éste el 83,4% de los 36.000 encuestados afirman usar programas anti-spam frente al 15% que no lo hace. La frecuencia de recepción semanal también ha sido objeto de análisis de la encuesta. Según ésta y por citar los datos más extremos el 1,3% de los 35.630 encuestados, esto es, 456 navegantes afirman no haber recibido nunca correo no deseado. Por el contrario 629 navegantes, el 1,8%, aseguran haber recibido más de 500 mensajes no solicitados semanalmente[43]. Asimismo el 37,6% asume como mejor medida prohibir y perseguir legalmente esta práctica, el 27,5% la creación de registro con direcciones de aquellos que no quieran recibir mensajes (listas Robinson) y el 23% la creación de una lista de empresas y/o personas que realizan estas actividades para filtrar mensajes. En cuanto al *phishing* el 50,1% afirma haberlos recibido y el 47,1% no.

Respecto de la relación entre el *spam* y el *phishing*[44] parece claro que este tipo de mensajes de distribución masiva puede ser una eficiente forma de captación

[41] La Sociedad de la Información en España 2009. Fundación Telefónica, 2009.

[42] Navegantes en la Red: 11ª encuesta a usuarios de Internet. AIMC, 2009

[43] Frecuencia de spam



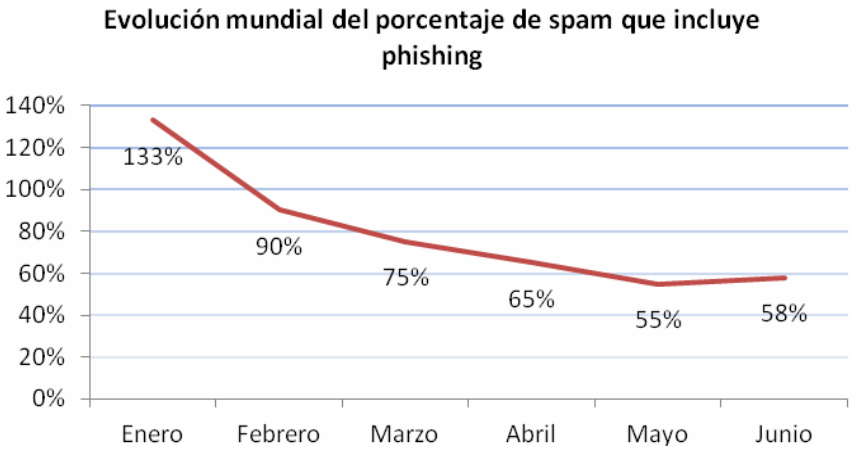
[44] correo electrónico que, utilizando una imitación de la página web de una empresa, induce al usuario final a facilitar datos confidenciales.

utilizada por los delincuentes. De hecho el correo electrónico es uno de los medios más habituales de contacto para la comisión de delitos informáticos. El porcentaje de mensajes *spam* que constituye *phishing* es bastante bajo pero es preciso tener en cuenta que éstos sólo abarcan una tipología de muy específica de fraude.

Aun así existe una tendencia hacia la reducción del porcentaje de *phishing* localizado en correos electrónicos no solicitados según datos recogidos del primer semestre de 2006[45].

Sigue asimismo en aumento la profusión, por correo electrónico o incluido en software, de programas espía que representan una grave amenaza para la privacidad de los usuarios porque vigilan y comunican el comportamiento en línea de un usuario y recogen información personal como contraseñas o números de tarjeta de crédito. La difusión de programas maliciosos como gusanos o virus facilita enormemente el envío de mensajes electrónicos no solicitados y una vez instalados permiten al infractor controlar el sistema informático objeto del ataque.

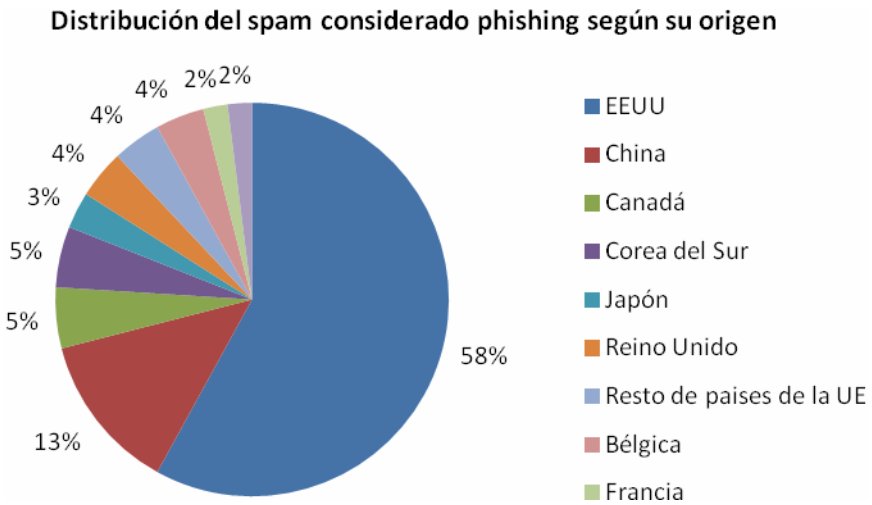
[45] Fuente: Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing. INTECO, 2007



En lo referido al origen del spam existe una elevada relación entre *spam* y *botnets* capturadas siendo habitualmente origen de este tipo de mensajes aquellos países con un mayor número de ordenadores controlados remotamente[46]. Por otro lado, dado que el mensaje intenta atraer la confianza del destinatario se intenta, en la mayoría de los casos, su envío desde lugares que generen confianza. De este modo, tal y como observamos en el gráfico, en la lista de grandes remitentes de spam con finalidad de fraude electrónico se encuentran EEUU y China.

Según el ***Informe anual de la sociedad de la información en España en 2008***[47], elaborado por la Secretaria de Estado de Telecomunicaciones y para la Sociedad de la Información dependiente del Ministerio de Industria, Turismo y Comercio, el correo no deseado afectaba al 49,5% entre los usuarios de Internet

[46] Fuente: Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing. INTECO, 2007



[47] La sociedad en Red 2008: informe anual, 2009.

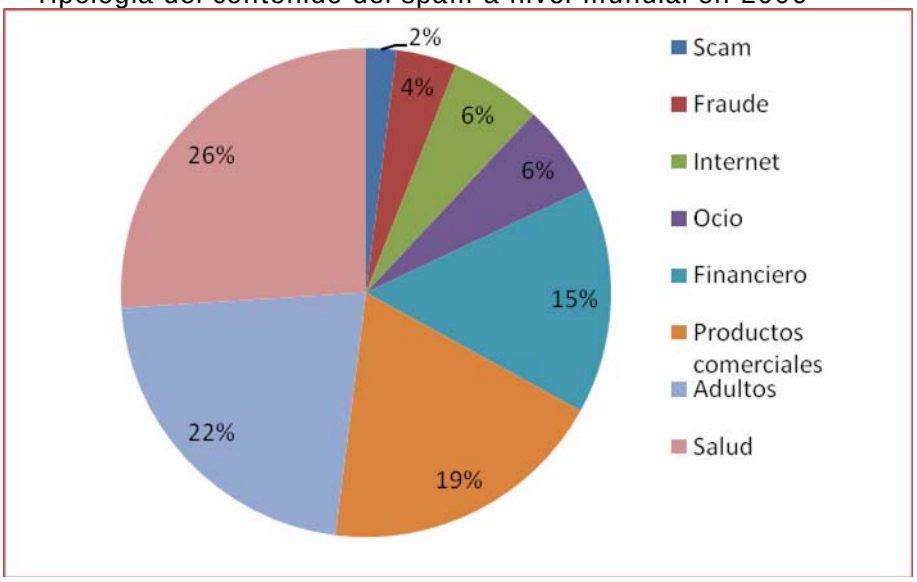
cuyo uso es habitual[48]. Para ese mismo trimestre el filtro anti-spam, sin embargo, era usado tan sólo por el 30,3% de los afectados.

Más allá del volumen de *spam* es necesario analizarlo como potencial herramienta delictiva. Como muestra el gráfico[49] aunque sólo un 4% de los mensajes aparece relacionado directamente con el fraude es preciso señalar que la apariencia de contenido financiero o comercial puede ser una simple máscara debajo de la cual se oculte una segunda fase de la estafa basada en la ingeniería social.

Junto a la problemática del spam existe lo que, por contagio, se ha venido a denominar el ***spamtelefónico***[50]: llamadas comerciales no solicitadas a través de la telefonía vocal fija o móvil. Una práctica que lejos de ser novedosa, resulta anterior al spam por correo electrónico y probablemente se esté acentuando en los últimos años. Quién no ha recibido alguna vez una llamada telefónica procedente de una línea sin identificar para ofrecer un servicio o producto. Una situación a la que el consumidor puede estar acostumbrado pero que no dejar de

[48] datos del tercer trimestre del 2008

[49] Tipología del contenido del spam a nivel mundial en 2006



[50] Gómez-Juárez Sidera, I. Consideraciones sobre el régimen jurídico del spam con ocasión del nuevo artículo 29.2 de la Ley de Competencia Desleal, 2010.

ser ciertamente molesta, especialmente a determinadas horas o si las llamadas son excesivamente reiteradas.

Con motivo de la celebración por primera vez del Día de Internet en España el 25 de octubre de 2005 la Agencia Española de Protección de Datos elaboró un decálogo con recomendaciones para combatir el spam, considerado problema considerable y creciente para los destinatarios de la SI: los usuarios las redes e Internet en general.

En España, como veremos posteriormente, la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico, en adelante LSSICE, prohíbe el envío de comunicaciones comerciales por correo electrónico no solicitadas, pero esta circunstancia no impide que los internautas vean inundados sus buzones de correos con spam procedente de otros países con una legislación más permisiva. Aunque la mayor parte del spam procede del exterior de la Unión Europea (se estima que el 80% del spam que reciben los españoles es norteamericano) son actualmente los países europeos los emisores del 25% de las comunicaciones no solicitadas enviadas.

La agencia asume la defensa de la privacidad de los usuarios de Internet frente al spam y establece un decálogo de recomendaciones para combatirlo y prevenirlo:

1. Ser cuidadoso al facilitar la dirección de correo electrónico
2. Utilizar dos o más direcciones de correo electrónico
3. Elegir una dirección de correo electrónico poco identificable para el spammer.
4. No publicar la dirección de correo en buscadores, foros, páginas web ni directorios de contactos. En caso de correos con direcciones múltiples en caso de envío ocultar las direcciones y en caso de reenvío eliminar las direcciones anteriores.

5. Leer detenidamente las políticas de privacidad y las condiciones de cancelación.
6. Sensibilizar a los niños en la utilización del correo y la mensajería instantánea.
7. No es conveniente contestar el spam porque informa de que la cuenta está activa y con seguridad se producirán más envíos. Sólo se deben responder de entre los correos recibidos fuera de España aquellos cuyo remitente sea conocido o confíe.
8. No pinche sobre los anuncios de los correo basura.
9. Utilice filtros de correo para separar el correo deseado del no solicitado.
10. Mantenga al día su sistema con antivirus actualizados y cortafuegos.

En su conjunto, la mayoría de medidas adoptadas en la Unión Europea y, que serán enumeradas con posterioridad, resultan insuficientes o no han sido capaces de paliar el problema del spam.

La razón puede atribuirse al funcionamiento en sí de las redes de comunicación basado en el protocolo de comunicación TCP/IP orientado específicamente a proporcionar la mayor conectividad posible entre equipos informáticos.

La contrapartida de esta notable y fundamental característica de Internet es su inseguridad estructural y la razón por la cual el correo electrónico basura, las intercepciones de las comunicaciones, los ataques contra los sistemas de información, el *spoofing* o robo de identidad o la difusión de virus, troyanos y gusanos tienen tal éxito.

De igual modo el coste marginal del medio a través del cual se difunden estos mensajes (correo electrónico) o mediante telefonía móvil (SMS y MMS), su posible anonimato, la velocidad con la que llega a los destinatarios y las

posibilidades en el volumen de las transmisiones se han aliado para la transmisión de spam se realice de forma abusiva e indiscriminada.

Costes del spam

A pesar de la idea bastante extendida entre los abonados y usuarios a los servicios del sector de las comunicaciones electrónicas que relaciona la existencia de publicidad con el acceso gratuito a recursos disponibles en línea, en Internet, el usuario es normalmente quien soporta el coste, en tiempo y dinero, de la aparición en el navegador de publicidad no consentida.

Investigar los casos de spam se convierte en una tarea cada vez más complicada. Los piratas informáticos ayudan a los emisores de spam en la ocultación de su verdadera identidad (*spoofing*). Su eliminación lleva tiempo y la proliferación y desarrollo de distintas técnicas fraudulentas que persiguen la apropiación indebida de datos personales, la transmisión de virus informáticos o la suplantación de la identidad tienen en el spam su canal de transmisión. Estas acciones ilícitas, consideradas delito en el ámbito de los ataques contra los sistemas de información en algunos países miembros, engloban el llamado delito informático o ciberdelincuencia[51]. Además, a menudo, induce a error y engaño. Pese a que su práctica ya es ilícita en virtud de las normas existentes en la Unión Europea sobre publicidad engañosa[52] y prácticas comerciales desleales una proporción considerable de spam parece responder a una voluntad de estafar a los consumidores.

Asimismo el spam constituye un serio problema para las empresas en forma de costes directos e indirectos. Los costes directos van desde la pérdida de

[51] Por ciberdelincuencia se entienden las actividades delictivas realizadas con ayudas de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas. En COM(2007) 267 final: Hacia una política general de lucha contra la ciberdelincuencia.

[52] Directiva 84/450/CEE sobre publicidad engañosa.

productividad (donde el personal se ve obligado a limpiar las bandejas de entrada y, por tanto, a reducir su rendimiento, a dificultar la búsqueda de mensajes realmente necesarios y a desbloquear, por saturado, el servidor de correo) hasta el gasto económico[53] que supone para proveedores de servicios de internet y proveedores de servicios de correo electrónico la inversión en tecnologías que amplíen las capacidades del ancho de banda de la red y de los servidores de correo y desarrollen técnicas de filtrado que eviten la entrada de spam en las bandejas de de correo.

Además, estas medidas de filtrado provocan costes indirectos tales como los *falsos positivos* entendidos como el correo comercial o profesional de interés que se deja de recibir y los *falsos negativos* como aquellos que por su vinculación con el spam dejan de leerse.

Puede suponer el colapso de los sistemas informáticos además de afectar a la reputación de los proveedores en la medida en que los usuarios lo pueden asociar a la lentitud de la navegación o a los fallos de conexión.

Tal es la problemática que se ha erigido en un negocio por sí mismo. Sus emisores alquilan o venden a las empresas listas con las direcciones de correo electrónico, previamente confeccionadas de modo ilícito, para sus fines comerciales. Especialmente lucrativo resulta el spam a través de redes de comunicación dado el enorme uso de éstas y el escaso coste que supone enviar una cantidad ingente de mensajes.

Desde la perspectiva individual constituye un problema porque invade de manera tenaz y persistente el espacio privado e íntimo de las comunicaciones, representa

[53] Se ha estimado que el coste en **2005** del spam ascendió a 39.000 millones de euros en el mundo y para las principales economías europeas a unos 3.500 millones en Alemania, 1.900 millones en el Reino Unido y 1.400 millones en Francia. Mientras se calcula en 11.000 millones de euros el impacto financiero de los programas espía y maliciosos. Fuente: Computer Economics: the 2005 malware report.

una intrusión a su intimidad. Como veremos, a través del envío de spam pueden lesionarse desde la privacidad e intimidad, en lo referido al tratamiento de datos personales, hasta la dignidad humana al vulnerar creencias o la protección frente a menores. Esta consideración preside las nuevas normas que regulan el marco de las comunicaciones comerciales.

La protección de datos de carácter personal y las comunicaciones comerciales

El desarrollo de nuevas tecnologías y el auge y mantenimiento del comercio electrónico precisan de la actuación de los sujetos que acceden a la red en condiciones de seguridad y buen nivel de conocimiento[54].

Sin embargo, este requerimiento se ve truncado por la desconfianza e inseguridad que generan en los internautas la realización de determinadas actividades como las transacciones electrónicas o los pagos electrónicos tan habituales en la vida cotidiana y, sin embargo, por realizarse enteramente a través de una máquina conectada a una red de proporciones incalculables generan por sí mismas una gran inseguridad, sobre todo, en lo referido al tráfico y tratamiento de datos de carácter personal.

Una práctica muy común vinculada al spam es la recolección de direcciones de correo electrónico, es decir, la recogida automática de datos personales en sitios web. Esta práctica es ilegal en virtud de la Directiva 95/46/CE sobre protección de datos personales y su libre circulación esté o no efectuada de manera automática con ayuda de un programa informático.

La relevancia que el tratamiento de los datos de carácter personal en general y los realizados con fines comerciales en particular tiene, para el avance y progreso de la actividad económico, social o cultural, lo ponen de manifiesto las

---

[54] Recordemos que la denominada *brecha digital* hace referencia a la diferencia socioeconómica entre aquellas comunidades que tienen accesibilidad a Internet y aquellas que no, aunque tales desigualdades también se pueden referir a todas las nuevas tecnologías de la información y la comunicación. También hace referencia a las diferencias que hay entre grupos según su capacidad para utilizar las TIC de forma eficaz, debido a los distintos niveles de alfabetización y capacidad tecnológica. También se utiliza en ocasiones para señalar las diferencias entre aquellos grupos que tienen acceso a contenidos digitales de calidad y aquellos que no.
Fuente: Wikipedia, consultable en http://es.wikipedia.org/wiki/Brecha_digital.

distintas normativas europeas y estatales aprobadas relativas a la protección de las personas físicas en lo referido al tratamiento de datos personales y a la libre circulación de éstos.

La protección de los datos constituye un principio importante para la Unión Europea. Además de en los artículos 6[55] y 30[56] del **Tratado de la Unión Europea** y el artículo 8[57] de la **Carta de los Derechos Fundamentales** se recoge 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 especialmente su derecho a la intimidad de forma que estos datos pueden circular libremente por la Unión Europea. Tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales estableciendo principios de orientación para determinar su licitud[58]. Dichos principios vienen recogidos en el artículo 17[59] y se refieren fundamentalmente al tratamiento de los datos que será efectuado de manera lícita y recogidos con fines determinados y además únicamente podrá realizarse si el afectado o titular de los datos da su consentimiento inequívoco. Además los interesados tendrán derecho a acceder a los datos y derecho a

[55] La Unión se basa en los principios de libertad, democracia y respeto de los derechos humanos y de las libertades fundamentales.

[56] 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.

[57] La protección de los datos personales constituye una de las libertades enunciadas.

[58]Protección de los datos personales
http://europa.eu/legislation_summaries/information_society/l14012_es.htm
[consultado el 02/07/2010]

[59] Los estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.

oponerse a su tratamiento con las excepciones y limitaciones establecidas relativas a la seguridad del Estado, seguridad pública, etc. Esta directiva general sobre el protección de datos se ve complementada por la Directiva sobre privacidad en las comunicaciones electrónicas que aplica los principios mencionados al tratamiento de los datos de carácter personal relacionados con la prestación de servicios de comunicaciones electrónicas disponibles para el público en las redes de comunicación pública.

Otras directivas relativas al tratamiento de datos personales son la **Directiva 97/66/CE** que traduce los principios establecidos por la anterior directiva en normas concretas para el sector de las telecomunicaciones y la **Directiva 2002/58/CE** que derogó la anterior para adaptarla al desarrollo de los mercados y las tecnologías de los servicios de las comunicaciones electrónicas para 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 las tecnologías usadas. Posteriormente fue 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 comunicaciones.

De hecho el marco legislativo comunitario sobre protección de datos y privacidad en Europa se diseñó con la idea de que la innovación tecnológica no lo dejara rápidamente obsoleto y resultase eficaz para la preservación de los derechos y las libertades en las modernas sociedades tecnológicas cada vez más dependientes del uso de las TIC, evitando así, que el tráfico de datos personales por la Red quede expuesto con más facilidad a mayores riesgos. Tanto es así que la normativa sobre protección de datos consiste en normas de protección de los

individuos cuyo objetivo es la defensa de la dignidad humana y la capacitación de los individuos para ejercer sus derechos y proteger sus intereses legítimos.

Las autoridades encargadas de su salvaguarda se enfrentan actualmente a grandes desafíos especialmente los derivados del frenético ritmo de los cambios tecnológicos: la tecnología evoluciona a una velocidad mayor de la que lo hacen las normas legales, la globalización de los datos hace especialmente difícil su control y se enfrenta a la extraterritorialidad en la aplicación de las normas, la comodidad que ofrecen los servicios de la SI puede llevar a una situación a veces irreversible de arriesgada despreocupación en lo referido a la vigilancia y seguimiento del tratamiento que se hace de los datos personales.

Respecto al marco normativo español tanto la Ley Orgánica de Protección de Datos, en adelante LOPD, como su reglamento de desarrollo tienen como objetivo principal garantizar y proteger el tratamiento de datos personales, las libertades públicas y los derechos fundamentales mediante el establecimiento de una serie de obligaciones para las entidades que realicen tratamiento de datos personales así como la puesta a disposición del afectado o interesado de herramientas adecuadas para la protección y ejercicio de su derecho.

La citada norma, aunque no lo refiere expresamente, considera la dirección de correo electrónico como dato personal[60]. Y ello con independencia de que la dirección de correo electrónico este compuesta por el nombre y/o apellidos de la cuenta de correo o por series numéricas o nombres de fantasía[61].

Según la Agencia Española de Protección de Datos cabrían varios supuestos:

---

[60] art.3: *a los efectos de la presente ley orgánica se entenderá por datos de carácter personal cualquier información concerniente a personas identificadas o identificables.*

[61] Plaza Soler, J.C. La regulación de los correos electrónicos comerciales no solicitados en el derecho español, europeo y estadounidense, 2002

- si la dirección estuviera compuesta por los nombres, apellidos y/o las iniciales del titular, con independencia del nombre del dominio al que esté vinculada la dirección, indudablemente sería un dato de carácter personal.
- si la dirección estuviera compuesta por un nombre de fantasía o una serie de caracteres alfanuméricos aleatorios siempre que el dominio vinculado a la dirección correspondiese al de la empresa donde trabaja el titular también se considera dato personal.
- si la dirección está compuesta por un nombre de fantasía o una serie de caracteres alfanuméricos aleatorios y el dominio es uno no vinculado a la empresa la agencia también lo considera dato personal dado que se puede acudir al servidor para verificar sin demasiada dificultad los verdaderos datos del titular.

Así las cosas el destinatario de toda comunicación comercial electrónica, en cuanto titular del dato personal que es la dirección de correo electrónico y de cualquier otro dato personal que haya dado origen al mensaje o esté contenido en el mismo, puede ejercer sobre tales datos los derechos de acceso, rectificación, cancelación y oposición.

En todo caso las direcciones de correo electrónico se someten a la protección regulada en la LOPD, a saber: la declaración de ficheros que contengan las direcciones de correo a la AEPD, el cumplimiento de los requisitos en la recogida de los datos previsto por el artículo 5 de la ley[62], la prohibición de tratamiento o cesión no consentidos de los datos y la limitación de las fuentes de recogida de datos con fines promocionales[63], es decir, los datos incluidos en el censo

[62] Derecho a información en la recogida de datos.

[63] art.30 LOPD: *quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades*

promocional y en las listas de personas pertenecientes a grupos profesionales o guías de servicios de telecomunicaciones.

Existen, no obstante, supuestos más ambiguos de recogida de direcciones de correo electrónico y de los cuales los spammers podrían sacar provecho. Tal es el caso de las direcciones captadas de sitios web. Los sitios web no son considerados, aunque puedan parecerlo puesto que el acceso a las páginas web es público, fuentes de acceso público y, en caso de considerarlas, tampoco se ajusta a la definición que la LOPD otorga a las fuentes de acceso público. Por tanto, a pesar de que el acceso es público, el uso de aplicaciones informáticas para recabar los datos es ilegal tal y como señala el artículo 4.7 de la LOPD *se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos*.

En el caso de direcciones de correo electrónico de personas físicas utilizadas en el marco de sus tareas institucionales o profesionales resulta incontestable que la puesta a disposición del público en general de las direcciones a través de páginas web o cualquier otro mecanismo se realiza a efectos exclusivos de comunicaciones concernientes con su actividad.

Por otro lado la elaboración de listados con direcciones de correo electrónico a modo de listín telefónico implica también el consentimiento previo de los titulares de los datos así como la obligación de informar del origen de los mismos y la identidad del responsable de su tratamiento. De este modo, si la dirección utilizada para el envío de spam ha sido sustraída de un fichero de este tipo, el

---

análogas utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o hayan sido facilitados por los propios interesados u obtenidos con su consentimiento. Posteriormente el reglamento de desarrollo de la LOPD *desarrolla este* artículo ampliando el ámbito de aplicación *a quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros* y precisa la finalidad del tratamiento de los datos a *finalidades determinadas, explicitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad* (art.45.1 del Real Decreto 1720/2007)

titular podrá ejercer su derecho de oposición al tratamiento de los datos contenidos en el fichero.

Asimismo el empleo de direcciones de correo electrónico obtenidas en foros y recursos similares es claramente un uso ilícito de los datos cuya finalidad para recabarlos fue distinta a la de su empleo para difundir publicidad.

Excluida, por tanto, la posibilidad de considerar lícitas las fuentes de acceso público para recabar los datos de contacto con fines de envío de correo electrónico, toda comunicación comercial, o está autorizada o es fruto de la excepción del artículo 21.2 de la LSSICE.

La LOPD no incluye el requisito del consentimiento expreso para el envío de publicidad por medios tradicionales sino que se conforma con que los datos hayan sido obtenidos legítimamente. Habla de consentimiento inequívoco del afectado requerido para el tratamiento de datos de carácter personal[64].

Conforme a lo anterior, se sitúa la práctica del spam contraria a la LOPD y otras leyes que regulan la actividad publicitaria y las actividades comerciales tanto por la forma que emplea para captar la información de direcciones personales de correo electrónico como por la forma de difundirla.

Ahora bien, ¿pueden ser de aplicación concurrente al envío de mensajes la LOPD y la LSSICE? Conforme al artículo 44[65] de la LSSICE es posible la concurrencia de procedimientos cuando las infracciones de la misma constituyan además, lesión de otros bienes jurídicos.

---

[64] art.6 LOPD

[65] Concurrencia de infracciones y sanciones: 3) *cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.*

Según Aparicio Vaquero[66] la regulación de las comunicaciones comerciales en la LSSICE se realiza a partir de su consideración como tratamiento de datos y, concretamente, como un supuesto especial del mismo en función de su finalidad, a saber, el envío de comunicaciones electrónicas y del instrumento o medio utilizado, el correo electrónico. Podrían aplicarse conjuntamente ambas normas sobre el mero envío si consideramos lesionados dos bienes jurídicos: los datos personales y la esfera personal en la cual irrumpe el correo.

Por tanto, la LOPD, en cuanto norma general, será de interés para la evaluación y dotación de contenidos de los términos empleado por la LSSICE en lo referente al consentimiento, derechos del destinatario y tratamiento de los datos personales y para la consideración de los datos de contacto como datos personales.

Por lo demás, la normativa española sobre comunicaciones comerciales se aplica a los emisores de las mismas establecidas en España y a los emisores residentes en otros países miembros de la UE cuando los destinatarios de las comunicaciones comerciales se encuentren en España.

Resultaría también de aplicación concurrente la LSSICE con cualquier otra normativa garante de otros bienes o derechos que resultasen infringidos. Tal es el caso de la protección de los consumidores y usuarios en relación a la informaciones contractuales o las de competencia desleal o publicidad engañosa.

[66] Aparicio Vaquero, J.C. Régimen jurídico de las comunicaciones comerciales realizadas a través del correo electrónico, 2005

La protección de los consumidores frente al spam

La resolución del Consejo de la Unión Europea sobre la dimensión relativa a los consumidores en la SI considera "que para instaurar esta confianza es necesario que exista en las nuevas tecnologías un nivel de protección equivalente al que rige en las transacciones tradicionales de los consumidores, aplicándose a los nuevos productos y servicios que ofrece la sociedad de la información los principios vigentes en materia de política de los consumidores, especialmente: la protección de los consumidores frente a las prácticas de comercialización no solicitadas, engañosas y desleales, incluida la publicidad, y el apoyo a que se pongan a disposición del consumidor medios fiables para filtrar el contenido de los sistemas de comunicación". Por tanto, el principio de tutela del ámbito de la privacidad de la persona se extiende a los destinatarios y usuarios de los servicios de la sociedad de la información.

La reciente Ley 29/2009 por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de la protección de consumidores y usuarios es fruto de la transposición al derecho español de la Directiva 2005/29/CE relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior. La citada Directiva tiene por objeto "*contribuir al buen funcionamiento del mercado interior y alcanzar un elevado nivel de protección de los consumidores mediante la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre las prácticas comerciales desleales que perjudican a los intereses económicos de los consumidores"*. Entre las prácticas comerciales consideradas desleales la Directiva contempla las prácticas comerciales agresivas entendiendo por tales "*toda práctica comercial que merme o pueda mermar de*

forma importante mediante el acoso, la coacción, incluido el uso de la fuerza, o la influencia indebida, la libertad de elección o conducta del consumidor medio con respecto al producto y le haga y le haga o pueda hacerle tomar una decisión sobre una transacción que de otra forma no hubiera tomado". En el anexo I cita expresamente en su condición de práctica comercial agresiva la realización de *proposiciones no solicitadas y persistentes por teléfono, fax, correo electrónico u otros medios a distancia.*

Así pues se introduce en la Ley de Competencia Desleal un nuevo artículo, el 29, que lleva por título *Prácticas agresivas por acoso*. De manera que conforme con lo establecido en su apartado 2[67] tendrán la consideración de prácticas comerciales desleales con los consumidores la realización de propuestas no deseadas y reiteradas por teléfono, fax, correo electrónico u otros medios de comunicación a distancia.

[67] *Igualmente se reputa desleal realizar propuestas no deseadas y reiteradas por teléfono, fax, correo electrónico u otros medios de comunicación a distancia salvo en las circunstancias y en la medida en que esté justificado legalmente para hacer cumplir una obligación contractual. El empresario o profesional deberá utilizar en estas comunicaciones sistemas que le permitan al consumidor dejar constancia de su oposición a seguir recibiendo propuestas comerciales. Para que el consumidor o usuario pueda ejercer su derecho a manifestar su oposición a recibir propuestas comerciales no deseadas, cuando éstas se realicen por vía telefónica, las llamadas deberán realizarse desde un número de teléfono identificable.*

Normas relativas al spam

La problemática derivada de la generalización del uso de Internet como escenario comercial y medio de difusión publicitario y de la apertura al mercado de las telecomunicaciones ha sido tenida en cuenta desde diversos organismos internacionales.

Como resultado de esta preocupación se han dictado a modo de recomendaciones una serie de principios generales relativos al comercio electrónico que afectan a la publicidad y las ofertas comerciales difundidas a través de la red y que han servido de guía para las posteriores redacciones de códigos deontológicos o de buenas prácticas.

También se ha necesitado un marco regulador de las comunicaciones electrónicas para la reforzar la competencia, facilitar la entrada en el mercado a nuevos operadores, estimular la inversión y en definitiva hacer más competitivo el sector de las comunicaciones electrónicas[68].

Este marco regulador de las redes y servicios de comunicaciones electrónicas[69] forma parte del paquete de Directivas que regulan las comunicaciones electrónicas en la Unión Europea[70]:

---

[68] Marco regulador de las comunicaciones electrónicas
http://europa.eu/legislation_summaries/information_society/l24216a_es.htm
[consultado el 02/07/2010]

[69] "*el prestado por lo general a cambio de una remuneración que consiste en su totalidad o principalmente en el transporte de señales a través de redes de comunicaciones electrónicas con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiofusión, pero no de servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; quedan excluidos los servicios de la sociedad de la información que no consistan en su totalidad o principalmente en el transporte de señales a través de redes de comunicaciones electrónicas*" En Directiva 2002/21/CE "Directiva marco"

[70] Directiva 2002/21/CE "**Directiva Marco**", Directiva 2002/20/CE "**Directiva de autorización**" a redes y servicios de comunicaciones electrónicas, Directiva 2002/19/CE "**Directiva de acceso**" a redes de comunicación electrónicas y recursos asociados y a su

- la ***directiva marco*** establece el marco regulador común a todas las redes y servicios de comunicaciones así como a los recursos asociados a ellos.
- la ***directiva de autorización*** garantiza la libertad de suministrar redes y servicios de comunicaciones electrónica.
- la ***directiva de servicio*** *universal* establece el conjunto mínimo de servicios de calidad especificada al que todos los usuarios finales tienen acceso, habida cuenta de las condiciones nacionales específicas, a un precio asequible sin distorsión de la competencia.
- la ***directiva de acceso*** tiene por objeto establecer un marco regulador para las relaciones entre los 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.
- la ***directiva sobre privacidad y comunicaciones electrónicas*** 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.

---

interconexión, Directiva 2002/22/CE "**Directiva de servicio universal**" a las redes y los servicios de comunicaciones electrónicas, Directiva 2002/58/CE "**Directiva sobre privacidad y comunicaciones electrónicas**" relativa a los datos personales y protección de la intimidad en el sector de las comunicaciones electrónicas.

Así las cosas, los sistemas para el control de las comunicaciones comerciales no consentidas o se confían, como veremos posteriormente, a la autorregulación cuyos principios y normas son recogidos en códigos éticos o de conducta o son reguladas por normas legales.

Básicamente son dos los sistemas para regular el spam: los que exigen el consentimiento expreso del receptor de correos electrónicos autorizando su envío (el sistema de **listas de exclusión *opt-out***[71]) y los que permiten el envío a cualquier destinatario siempre que no haya manifestado su voluntad expresa de recibirlo (el sistema de **listas de inclusión *opt-in***[72]). La opción por uno u otro sistema se debe a razones de mera política legislativa y a la presión ejercida por los grupos de intereses en juego[73].

Mediante las **listas de exclusión** el destinatario debe incluirse en dichas listas para no recibir correo comercial. No cabe duda que este sistema beneficia a los anunciantes puesto que les asegura poder llegar a un número mayor de destinatarios. Las empresas pueden enviar comunicaciones comerciales pero deben consultar periódicamente dichas listas y no incluir en sus envíos publicitarios a aquellos inscritos.

Dos son los procedimientos de elaboración de estas listas: por medio de listas públicas a nivel nacional o por medio de listas privadas múltiples. En el primer caso, el más cómodo, el usuario deberá inscribirse en una sola lista. En el

---

[71] envío no autorizado de mensajes comerciales a una lista de correo electrónico constituida por internautas que no han dado su acuerdo explícito a la recepción de tales mensajes pero que tienen la posibilidad de retirarse de la lista. En este sistema, el acuerdo del internauta está implícito.

[72] envío autorizado de mensajes comerciales a una lista de correo electrónico constituida por internautas que han dado su acuerdo previo a la recepción de tales mensajes publicitarios. En este sistema, el acuerdo del internauta está explícito.

[73] Aparicio Vaquero, J.C. Régimen jurídico de las comunicaciones comerciales realizadas a través del correo electrónico, 2005

segundo caso los usuarios deberán inscribirse en todas y cada una de las listas manifestando así el rechazo a recibir comunicaciones comerciales no solicitadas. Este sistema hace necesario en el momento de enviar una mensaje publicitario no consentido informar de dónde proceden los datos de la cuenta de correo. De este modo, debe informarse al interesado cómo acceder a dichas listas y así no autorizar envíos futuros.

Una parte de los partidarios del sistema de listas de exclusión voluntaria sostiene que el derecho de oposición debe ejercerse únicamente frente a quien ha enviado el mensaje no solicitado. Por otro lado, hay quien promueve un mecanismo de listas de exclusión, nacionales o internacionales, en el que pueda inscribirse quien lo desee, antes o después de haber recibido mensajes no solicitados. En este caso son los responsables de los envíos quienes deben consultar regularmente dichas listas a fin de respetar el deseo expresado por los inscritos en ellas[74].

Los ficheros de exclusión del envío de comunicaciones comerciales se conocen popularmente como ***listas Robinson*** término, cuyo origen discutido, parece ser el apellido de la primera persona que solicitó no recibir comunicaciones de carácter comercial. Por tanto, el servicio de listas Robinson tiene por objeto 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 la forma de mailing dirigido personalmente a ellos. Aquellas personas que por el contrario deseen recibir más envíos publicitarios también podrán solicitarlo al servicio de listas Robinson y formar parte de manera gratuita de la Lista de Preferencia.

[74] Gómez-Juárez Sidera, I. Consideraciones sobre el régimen jurídico del "spam" con ocasión del nuevo artículo 29.2 de la Ley de Competencia Desleal, 2010.

En la actualidad existe únicamente un fichero común de exclusión publicitaria al amparo de lo dispuesto en el artículo 49 del Real Decreto 1720/2007[75] si bien nada impide la creación de otros. Tal es el caso de la Federación de Comercio Electrónico y Marketing Directo que introdujo, hace más de 14 años cuando las comunicaciones comerciales se realizaban casi exclusivamente por correo postal, el denominado servicio de listas Robinson destinado a restringir la publicidad no deseada que reciben los ciudadanos a través del medio de comunicación que elijan[76].

Mediante las **listas de inclusión** se autoriza el envío de publicidad únicamente a aquellas personas que previamente y de forma expresa han manifestado la voluntad de recibirla. Este sistema beneficia a los usuarios al respetar sus voluntades de no recibir comunicaciones comerciales no solicitadas porque en caso contrario se vería vulnerado el derecho a la privacidad y las molestias de saturación de servidores de correo. Pese a todo si la medida sólo se adopta a nivel nacional únicamente protege a los envíos dentro del país y no aquellos procedentes de otros con una normativa diferente.

Por éste sistema, el de listas de inclusión opt-in y, después de varias directivas aprobadas apostando por uno u otro sistema o dejándolo en manos de los países como veremos, parece responder final y decididamente el criterio europeo actual.

---

[75] Por el que se aprueba el Reglamento de desarrollo de la ley orgánica 15/1999 de protección de datos de carácter personal: *será posible la creación de ficheros comunes, de carácter general o sectorial, en los que son objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.*

[76] Reglamento del fichero de lista Robinson. Disponible en: https://www.listarobinson.es/reglamento_01.asp, consultado el [2/08/2010]

La **Directiva 97/7/CE**[77] constituye la primera referencia normativa sobre las comunicaciones comerciales no solicitadas con finalidad comercial. Para el tema que nos ocupa tendrán especial vinculación los siguientes considerandos:

- considerando 12: en el caso de las comunicaciones telefónicas resulta apropiado que el consumidor reciba suficiente información al comienzo de la conversación para decidir si continúa o no.
- considerando 16: el envío promocional de un producto o servicio al consumidor sin petición previa o acuerdo explícito por parte de éste siempre que no sea suministro de sustitución no puede admitirse.
- considerando 17: trae a colación los artículos 8 y 9 del Convenio Europeo para la protección de los derechos humanos y las libertades fundamentales y procede a reconocer al consumidor el derecho a la protección de la vida privada en particular frente a ciertas técnicas de comunicación especialmente insistentes y a la adopción de medidas por parte de los estados miembros para proteger de forma eficaz a aquellos consumidores que no deseen ser contactados por medio de estas técnicas invasivas. En el caso de comunicaciones telefónicas deberá precisarse explícita y claramente al principio de cualquier conversación con el consumidor la identidad del proveedor y la finalidad comercial de la llamada.

Ya en su articulado el 10 dispone que la utilización por un proveedor de técnicas de comunicación a distancia tales como el sistema automatizado de llamada sin intervención humana y el fax necesitan el consentimiento previo del consumidor. Los estados miembros velarán porque otras técnicas distintas de las

[77] 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.

mencionadas cuando permitan una comunicación individual solo se utilicen a falta de oposición manifiesta del consumidor.

Es decir, el envío queda regulado por el sistema opt-out que permite el envío de publicidad por correo electrónico si no ha habido oposición expresa del destinatario.

Posteriormente la Cámara de Comercio Internacional (CCI) publicó en 1998 los ***Principios generales sobre la publicidad y marketing en Internet*** donde exige el respeto a los principios de legalidad en el país de origen, a saber, veracidad, decencia y honestidad de la publicidad así como la identificación de la publicidad como tal y la identificación inequívoca del anunciante. Asimismo se hace especial referencia a los derechos que asisten a los internautas en orden a su privacidad.

Por otro lado la Organización para la cooperación y desarrollo económico (OCDE) aprobó ese mismo año las ***Directrices sobre la protección del consumidor en el contexto del comercio electrónico*** donde hizo hincapié en la necesidad de conseguir la confianza del usuario en el entorno electrónico garantizando la seguridad de las redes y de los sistemas de información.

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

En el año 2000 fue aprobada la **Directiva 2000/31/CE**[78] sobre el comercio electrónico. Su objetivo es 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 lo cual establece el principio de control en origen[79] de dichos servicios, comunicaciones comerciales, entre otros, y excluye de su aplicación las comunicaciones comerciales no consentidas. También establece modos de protección contra el correo electrónico no solicitado dejando abierta la aceptación o no del envío de comunicaciones comerciales no solicitadas al optar por el sistema opt-out o de listas de exclusión voluntarias en su exposición de motivos y considerandos: *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 lo está, en particular, por las Directivas 97/7/CE y 97/66/CE*[80]*. 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 identificadas como tales con el fin de mejorar la transparencia y facilitar el funcionamiento de los dispositivos*

[78] 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 el comercio electrónico en el mercado interior.

[79] El control en origen implica que el mensaje publicitario se somete a la normativa del estado de procedencia del mismo. El control en destino supone que el mensaje emitido deberá adecuarse al ordenamiento jurídico del estado receptor del mismo.

[80] Sólo se refiere en su artículo 12 a los sistemas de llamada automática sin intervención humana o fax.

creados por la industria. Los estados miembros que permiten el envío de comunicaciones comerciales no solicitadas por parte de prestadores de servicio en su territorio por correo electrónico sin consentimiento previo del receptor, deben garantizar que los prestadores de servicios consulten periódicamente las listas de exclusión voluntarias en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y las respeten[81].

Ya en su articulado el 7 permite a los estados miembros decidir si prohíbe o no el envío de spam y regula en caso afirmativo los requisitos que deberán cumplir: la identificación del mensaje como correo no solicitado y el respeto a las listas de exclusión voluntarias.

Como vemos la Directiva no ofrece excesiva información en torno a cómo debe hacerse este control, no establece los plazos en los que obligatoriamente deberán consultarse las listas de exclusión o si el sistema deberá ser de listas públicas o privadas ni bajo qué condiciones. Asimismo deja claro que existe la posibilidad de prohibir rotundamente esta práctica publicitaria al afirmar "*los estados miembros que permiten el envío"…*

Entre las excepciones al principio de control en origen declara la licitud de las comunicaciones comerciales no solicitadas, por tanto, esta materia queda sometida a la legislación del país destinatario.

Aunque comparte elementos comunes con la legislación norteamericana contiene obligaciones más difusas que aquélla[82]. Así, no establece ninguna palabra común para todos los estados miembros que deba figurar en el encabezamiento del mensaje y no obliga a que la identificación conste en el espacio destinado al

[81] Considerandos 30 y 31 de la Directiva 2000/31/CE

[82] Plaza Soler, J.C. La regulación de los correos electrónicos comerciales no solicitados en el derecho español, europeo y estadounidense, 2002

asunto del correo electrónico. No obliga a que el remitente aporte una dirección de correo electrónico válida y funcional a la que el destinatario pueda dirigir su deseo de no recibir más correo comercial como tampoco obliga a incluir en los mensajes enlaces a las listas de exclusión. Tampoco se incluye en la Directiva referencias a contenidos de carácter pornográfico o dirigido a menores ni la prohibición de incluir títulos o contenidos falsos en los mensajes.

Se ha incorporado al ordenamiento jurídico español por medio de la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico cuyo objetivo es generar confianza y seguridad en el entorno de las telecomunicaciones y, su principal finalidad, como veremos en el capítulo dedicado al sistema normativo español, regular el régimen jurídico de los servicios de la sociedad de la información y de la contratación en red.

Como apuntábamos, la legislación vigente hasta ahora en Europa era bastante pendular con normas que recogían el principio *opt-in* y otras que se inclinaban por el principio *opt-out*. Sin embargo, mientras que este segundo principio había sido el más reconocido a nivel europeo, la postura restrictiva del *opt-in* parece haber triunfado definitivamente en la **Directiva 2002/58/CE**[83] que modifica las Directivas 97/7/CE y 97/66/CE.

La mencionada directiva, aprobada en 2002, sobre la privacidad y las comunicaciones electrónicas 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 de forma previa por su destinatario.

[83] 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.

Concretamente, el artículo 13[84], 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. El punto común de estos países es este artículo y tiene como finalidad establecer un marco intraeuropeo eficaz en el intercambio de información en denuncias sobre spam.

La entrada en vigor de este artículo ha unificado el mercado de la Unión Europea adoptando de forma obligatoria la necesidad de obtener el consentimiento previo para enviar comunicaciones comerciales no solicitadas con independencia del medio utilizado. El consentimiento[85] puede darse de varias maneras ya que la Directiva no establece de forma específica el método efectivo para obtenerlo. Así el considerando 17 afirma que *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 en un sitio web en Internet.* No obstante, no obliga al remitente a dar una dirección de correo electrónico válida para que el destinatario pueda exigirle la no inclusión en su lista de destinatarios ni a enlazar a las listas de exclusión, como tampoco quedan prohibidos todos los

[84] Requiere que antes de utilizar aparatos de llamada automática, el fax o el correo electrónico, incluidos los SMS, con fines de venta directa, los abonados hayan dado su consentimiento.

[85] Consentimiento del interesado: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan. En art.2) h de la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos)

mensajes electrónicos no solicitados por el denominado consentimiento previo suave[86].

El punto 2 del artículo 13 establece una excepción al consentimiento previo: en el contexto de la venta de un producto o servicio previo el remitente podrá usar la dirección de correo sin consentimiento previo siempre y cuando el contenido del envío publicitario esté relacionado con productos o servicios similares a los de la relación contractual y se facilite siempre el derecho de oposición al tratamiento de sus datos gratuitamente y de modo simple.

En este sentido el Grupo de Trabajo del Artículo 29[87] sobre protección de datos se ha pronunciado en relación a 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 Directiva 2002/58/CE. Esto implica que los mensajes comerciales solo podrán ser enviados a aquellos que hayan brindado sus datos de contacto dentro de la venta de un producto o servicio, lo que requerirá que se tome en cuenta el periodo de tiempo durante el cual el consentimiento pueda ser considerado como válido y permita el envío de mensajes. Sólo la persona natural o jurídica que haya recolectado los datos se encuentra facultada para enviar correos electrónicos comerciales. No obstante, la limitación al marketing de productos o servicios similares, es reconocida por el Grupo del Artículo 29 como un concepto de difícil aplicación práctica.

[86] Plaza Soler, J.C. La regulación de los correos electrónicos comerciales no solicitados en el derecho español, europeo y estadounidense, 2002.

[87] creado en virtud del artículo 29 de la Directiva 95/46/CE de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.

El punto 3[88] 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 bien sin el consentimiento previo bien respecto de los abonados que no deseen recibir dichas comunicaciones (*listas de exclusión*) y deja en mano de los estados en el momento de la transposición de la Directiva a su legislación la elección entre estas dos posibilidades.

El punto 4 prohíbe para todas las categorías de destinatarios (personas físicas y jurídicas) prohíbe el envío de mensajes de venta directa que oculten o disimulen la identidad del remitente. Los mensajes deben mencionar una dirección válida a la que el destinatario pueda enviar una petición de oposición.

Pese a la transposición del texto comunitario a la Ley General de Telecomunicaciones el legislador español no hizo mención de la ilicitud del ocultamiento, falsificación o inexactitud que sometiera al destinatario a error en cuanto a la dirección del mensaje o la identidad de su iniciador. Sin embargo dicha carencia podría quedar salvaguardada en cierta medida por el artículo 20.1 de la LSSICE y deducirse de frases de su enunciado tales como «los prestadores de servicios deberán facilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado».

Finalmente, el punto 5[89] 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 (personas jurídicas) [90].

---

[88] *Los Estados miembros tomarán las medidas adecuadas para garantizar, que, sin cargo alguno, no se permitan las comunicaciones no solicitadas con fines de venta directa en casos que no sean los mencionados en los apartados 1 y 2, bien sin el consentimiento del abonado, bien respecto de los abonados que no deseen recibir dichas comunicaciones. La elección entre estas dos posibilidades será determinada por la legislación nacional.*

[89] *Los apartados 1 y 3 se aplicarán a los abonados que sean personas físicas. Los Estados miembros velarán asimismo, en el marco del Derecho comunitario y de las legislaciones*

Meses más tarde de ese mismo año 2002 se aprueba la **Directiva2002/65/CE**[91] que amplía el consentimiento previo al prever en su artículo 10 las siguientes restricciones a las comunicaciones no solicitadas: consentimiento previo en caso de comunicaciones no solicitadas por medio del fax y llamadas automáticas y para técnicas de comunicación individual distintas a las enumeradas no autorizadas sin consentimiento previo o únicamente utilizadas si no ha habido oposición manifiesta.

Mientras el Derecho hace lo que puede para afrontar un fenómeno de naturaleza indudablemente mundial anclado en su ancestral principio de territorialidad en la aplicación de sus normas y sin una legislación internacional en la materia, los tecnólogos, hartos de estos mensajes que saturan servidores e implican costes económicos directos e indirectos, deciden poner barreras con mayor o menor fortuna. De este modo los técnicos hablan de tres medidas de protección que dependerán de la fase en que se adopten[92]:

- Las medidas precavidas son aquellas que contribuyen a no distribuir spam dentro de las propias organizaciones por medio de la aplicación de códigos de conducta, el correcto mantenimiento de los equipos y la formación e información adecuada de los empleados.
- Las medidas reactivas son aquellas dirigidas a cada usuario para que en caso de recibir spam lo elimine con el menor esfuerzo posible.

---

nacionales aplicables, por la suficiente protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a las comunicaciones no solicitadas.

[90] Plaza Soler, J.C. La regulación de los correos electrónicos comerciales no solicitados en el derecho español, europeo y estadounidense, 2002.

[91] 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.

[92] Plaza Soler, J.C. Los correos electrónicos comerciales no solicitados un año después de la LSSICE. 2004.

- Las medidas preactivas son aquellas adoptadas antes de que lleguen a los ordenadores, es decir, desde propios los servidores de correo.

Se incluyen entre las medidas reactivas y preactivas:

- Los filtros basados en **listas negras**: son los más antiguos de todos y quedan constituidos en base a un número variable de denuncias de los destinatarios de spam contra los servidores desde los cuales es enviado. Los servidores a través de los cuales se envía spam son incluidos en una lista negra y bloqueados por el administrador de la lista. Una vez que estos servidores ingresan en una lista negra y sus usuarios no spammers no pueden enviar correos se ponen en contacto con el administrador del servidor de modo que pueda ofrecer nuevamente servicios a sus clientes siempre y cuando consiga ser eliminado de lista procedimiento no demasiado fácil porque dependerá de la subjetividad del administrador de la lista. Por otro lado la confección de estas listas suponen el almacenamiento de datos personales tanto de spammers como de denunciantes y no siempre suficientemente protegidos.

  Un ejemplo de esta lista es la lista negra PUAS (plataforma unificada anti-spam) avalada por la comunidad científica española RedIris.

- Los filtros basados en **listas blancas** únicamente permiten los mensajes de los servidores de correo en los que confía el destinatario o en los mensajes procedentes de su libreta de direcciones. Exige, por tanto, la personalización absoluta de la cartera de direcciones puesto que el titular de la dirección de correo decide en quién confía o no pero al mismo tiempo que los hace demasiado restrictivos también resultan poco prácticos. No obstante pueden llegar a ser tan subjetivas como las listas negras si las direcciones de confianza no son elegidas por el propio usuario.

- Los filtros **bayesianos** o filtros **adaptativo**s no clasifican como los anteriores los mensajes por su dirección de procedencia IP sino por las palabras que contienen y su frecuencia. Cuando llega un mensaje el filtro compara su contenido con un lista de palabras no aceptadas analiza el contexto y calcula la probabilidad de que sea spam. Evolucionan con el spam de modo que si cambian las palabras los filtros lo reconocen automáticamente. Sin embargo no evitan el problema básico: que los servidores de correo se colapsen.

El sistema normativo español

El problema que plantea Internet es la ausencia de una regulación internacional unificada. Además, tal y como viene expresado por la LSSICE en su exposición de motivos, su implantación tropieza con algunas incertidumbres jurídicas que es preciso aclarar con el establecimiento de un marco jurídico adecuado que genere en todos los actores intervinientes 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 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 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 ya se cuenta con una normativa específica como ya hemos visto. En el caso español 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 especificidades de la publicidad en este nuevo medio.

Pues bien, 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.

En segundo término la Constitución Española impone la integración en el ordenamiento jurídico interno de las normas emanadas de las instituciones

comunitarias. En este sentido las directivas ya enumeradas han regulado las comunicaciones comerciales surgidas del nuevo entorno.

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 los 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.

En España la norma que está destinada a regular por primera vez el correo electrónico comercial es la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, en adelante, LSSICE. Su objetivo, generar confianza y seguridad en el medio electrónico.

Incorpora al ordenamiento jurídico español la Directiva 2000/31/CE. Es aplicable, siguiendo el principio de control en origen, a los prestadores de servicios de la sociedad de la información establecidos en España[93]. Pero como excepción al principio de control en origen, al igual que la norma comunitaria, declara su aplicación a los prestadores de servicios establecidos en otro estado miembro de la UE o del Espacio Económico Europeo (EEE) cuando el destinatario de los servicios radique en España y los servicios afecten a diversas materias, en ellas, la licitud de las comunicaciones comerciales no solicitadas[94] por correo

[93] LSSI, art.2: *Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.*

[94] LSSI, art.3: *a los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se*

electrónico u otro medio de comunicación electrónica equivalente o aun cuando estando fuera del territorio de la UE o del EEE los principios normativos españoles no contravengan lo dispuesto en los Convenios Internacionales.

De este modo el envío de spam que desde España se lleve a cabo a otros estados miembros ha de adecuarse a la LSSICE en base al control en origen. Cuando la remisión de spam procede de prestadores de servicios establecidos en la UE o el EEE y el destinatario esté en España se aplica el principio de control en destino. Así, la regulación de spam está garantizada por la LSSICE sobre la base de los dos principios reguladores de modo que los destinatarios de spam estarán protegidos de remisiones no consentidas procedentes de países pertenecientes o no a la UE o el EEE[95].

La LSSICE regula las comunicaciones comerciales estableciendo que éstas y las ofertas promocionales se regirán, además de por la misma, por su normativa propia y la vigente en materia comercial y de publicidad. Asimismo se declara expresamente la aplicación de la LOPD especialmente en lo que se refiere a la obtención de los datos personales, información de los interesados y creación y mantenimiento de ficheros.

Se recoge el principio de identificación de la publicidad tanto para el anunciante como para el mensaje que contenga la comunicación comercial[96].

---

haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica. La utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador.

[95] En opinión de Vázquez Ruano esta protección aumentada es innecesaria dada la tendencia de los países comunitarios a la prohibición de envíos publicitarios no consentidos.

[96] "*toda forma de comunicación dirigida a la promoción directa o indirecta, de la imagen, de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional*. Prosigue el texto ampliando la definición con *no tendrán consideración de comunicación comercial los datos que*

En el caso de las comunicaciones realizadas a través de correo electrónico, la identificación del mensaje publicitario deberá constar incluyendo al comienzo de la misma la palabra *publicidad*[97]. En los supuestos de ofertas promocionales que incluyan descuentos, premios, regalos, etc., además de su identificación inequívoca en cuanto al tipo de promoción, deberá cumplir la normativa existente en materia de ordenación del comercio. Por tanto, prevé un régimen general aplicable a la actividad publicitaria ejercida a través de medios electrónicos y otro particular referido a la remisión promocional a las cuentas de correo electrónico o medios análogos.

En su artículo 21.1 prohíbe de forma expresa el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente[98] que previamente no hubieran sido

---

permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, servicios, o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica". LSSICE. Anexo.
Como observa Rivero González la definición de comunicación comercial abarca todo tipo de comunicaciones en línea con independencia del formato y soporte, lógicamente, con finalidad comercial o empresarial. Por el contrario no se consideran comunicaciones comerciales los mensajes difundidos con finalidad informativa, la publicidad institucional destinada a fomentar determinadas conductas sociales ni la propaganda política o religiosa por perseguir no la promoción de bienes y servicios sino la adhesión a una ideología o creencia.

[97] o la abreviatura *publi*. Modificación incorporada por la Ley 56/2007 de Medidas de Impulso de la Sociedad de la Información.

[98] En este sentido, el Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE, adoptado por el Grupo del artículo 29 de protección de datos el 27 de febrero de 2004, señala que *"… los servicios abarcados actualmente por la definición de correo electrónico incluyen: el correo basado en el protocolo SMTP (Simple Mail Transport Protocol), es decir, el "correo electrónico" clásico; el servicio de mensajes cortos SMS (el considerando 40 de la Directiva 2002/58/CE clarifica que el correo electrónico incluye los SMS); los servicios de mensajes multimedia MMS; los mensajes en contestadores; los sistemas de mensajería vocal incluidos en los servicios móviles; y las comunicaciones enviadas por Internet dirigidas directamente a una dirección IP. Los boletines enviados por correo electrónico también están incluidos en esta definición. Esta lista no puede considerarse exhaustiva y puede necesitar ser revisada habida cuenta de los avances del mercado y de la tecnología".*

solicitadas o expresamente autorizadas por los destinatarios de las mismas. Esta prohibición encuentra su excepción en el segundo párrafo del artículo que autoriza el envío cuando exista una relación contractual previa, se obtengan lícitamente los datos de contacto del destinatario y se refiera a productos similares. En cualquier caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines comerciales mediante un procedimiento sencillo y gratuito tanto en el momento de recogida de los datos como en cada una de las comunicaciones posteriores dirigidas. Así 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. En la actualidad, se viene aplicando por las empresas remitentes de correspondencia exigiendo a los destinatarios que la petición de rectificación o cancelación de datos se le remita mediante carta certificada o fax, con coste, por tanto, para el solicitante pero no cobrándole en concepto de tratamiento de los datos[99].

Es necesario recordar que inicialmente no contemplaba esta excepción y exigía en todo caso el consentimiento previo del destinatario incluso en aquellos supuestos en los que existiese una relación contractual previa tal y como establecía en su redacción anterior el artículo 22. Con el fin de adecuar el régimen de consentimiento previo de la LSSICE al recogido en la Directiva 2002/58/CE se incorporó la mencionada excepción. En opinión de Vázquez Ruano esta norma *limita el ejercicio publicitario en línea no solicitado en mayor medida que si se ejerce por los canales de comunicación convencionales*[100]. Más aún si

[99] Plaza Soler, J.C. La regulación de los correos electrónicos comerciales no solicitados en el derecho español, europeo y estadounidense, 2002

[100] Vázquez Ruano, T. La protección de los destinatarios de las comunicaciones comerciales electrónicas, 2008.

se tiene en cuenta que en esta práctica comercial existen dos fases diferenciadas. En la primera respecto de la información personal necesaria para el envío de comunicaciones comerciales, la dirección de correo electrónico, se precisa el deber de información, la voluntad inequívoca del titular de los datos que en algunos casos cuando la finalidad es comercial la conformidad se presume. En la segunda, referida al envío publicitario en sí mismo limitado, sólo la necesidad de consentimiento previo pero olvida los requisitos del contenido publicitario, la cantidad de mensajes que se envían o la intencionalidad del envío. Asimismo surgen, entre los juristas, algunas imprecisiones en torno a este articulado que no obstante sí pueden ser precisadas con la normativa homóloga norteamericana tales como ¿qué debe entenderse por relación contractual previa?, ¿qué productos o servicios adquieren el apelativo de similares a los que fueron inicialmente contratados con el cliente?, ¿atiende la similitud al precio, la calidad, el estilo o su destino, entre otros?, ¿a qué momento nos debemos remontar para determinar el inicio de la relación contractual?, ¿la relación debe nacer en el ámbito de la contratación electrónica o requiere la perfección del contrato para hablar de relación contractual previa? [101]

La LSSICE adopta un sistema de listas de inclusión (*opt-in*). La prestación del consentimiento[102] expreso requiere la actitud proactiva o la manifestación de una voluntad libre, inequívoca y fundada de quien cede los datos. No hay que olvidar que la dirección de correo electrónico es un dato de carácter personal y, como tal, el consentimiento es el definido por la LOPD que coincide exactamente con el

---

[101] Guillén Catalán, R. Spam y comunicaciones comerciales no solicitadas, 2005.

[102] considerando 17 de la Directiva 2002/58/CE: el consentimiento debe tener el mismo significado que el recogido en la Directiva 95/46/CE, a saber, toda manifestación de voluntad, libre, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que lo conciernan.

definido por la Directiva 95/46/CE. Éste puede recabarse en el marco de un procedimiento de contratación o suscripción a algún servicio que tenga lugar vía web y en el que el destinatario deba facilitar su dirección de correo incluyendo en las condiciones generales de contratación y, distinguido del resto de contenido, una cláusula sobre el consentimiento del destinatario a la recepción de comunicaciones comerciales o bien ofreciendo la posibilidad de facilitar la dirección de correo para recibir información sobre los productos o servicios ofrecidos por la empresa mediante un mensaje y un formulario tipo incluido en la página web de la empresa.

Por el contrario no serán válidos los consentimientos tácitos y, en cualquier caso, siempre que se requiera el consentimiento quien lo recabe deberá informar al usuario de la finalidad del mismo, de manera que si la finalidad es utilizar el correo electrónico para hacer publicidad de sus productos deberá ser notoria dicha pretensión. De igual modo son ilícitas peticiones genéricas para autorizar la recepción de publicidad en abstracto del tipo *a efectos de envíos publicitarios* porque el consentimiento otorgado ha de ser específico[103].

Por otro lado el consentimiento informado exige sólo que el titular de los datos sea informado del destino de éstos y no se oponga a su cesión.

Por último, en cuanto a los derechos que asisten al destinatario de los envíos, el artículo 22, modificado por la Ley 32/2003 General de Telecomunicaciones, establece que 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.

En lo referido al **régimen sancionador** el carácter masivo y el respeto a la protección de datos de carácter personal han sido los fundamentos tomados en

[103] Aparicio Vaquero, J.C. Régimen jurídico de las comunicaciones comerciales realizadas a través del correo electrónico, 2005.

cuenta al normalizar la prohibición del spam. En la ley hasta el apartado correspondiente a infracciones y sanciones no se hace presente el carácter masivo.

Son **infracciones graves**, que prescriben a los dos años, el envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónico equivalente o el envío en el plazo de un año de más de tres comunicaciones a destinatarios que no lo hayan autorizado o se hayan opuesto. Por tanto establece en dos las causas de ilicitud: por un lado el envío masivo cuando no exista consentimiento previo y expreso del destinatario o bien cuando en el contexto de una relación comercial previa el destinatario se oponga al uso de sus datos para tratamiento con fines comerciales y promocionales y por otro el envío reiterado consistente en el envío en el plazo de un año de más de tres comunicaciones comerciales no autorizadas a un mismo destinatario. Si se envían menos de tres mensajes se incurre en infracción leve con multas de hasta 30.000 euros, las multas para las infracciones graves oscilan entre los 30.001 y los 150.000 euros.

También es infracción grave el incumplimiento significativo tanto de la obligación del emisor[104] establecida en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios[105] como de la establecida[106] sobre la información y rechazo del tratamiento de los datos.

---

[104] art. 22.1 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. A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieren prestado. Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.*

[105] art.38.3)d de la LSSICE: *la utilización de los datos retenidos, en cumplimiento con del artículo 12, para fines distintos a los señalados en él.*

[106] art.22.2 de la LSSICE: *cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los*

Son **infracciones leves** el envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónico equivalente a los destinatarios que no hayan autorizado su remisión o se hayan opuesto a ella cuando no constituyan infracción grave.

Como vemos, del mismo modo que la LSSICE considera el envío no consentido de comunicaciones comerciales sancionable desde el punto de vista administrativo con sanciones pecuniarias también la LOPD considera la captación ilícita de la dirección de correo electrónico una infracción administrativa y no penal.

Dado el carácter transnacional del spam cuando el emisor se encuentre fuera de la UE o del EEE, las autoridades nacionales pueden ordenar a los prestadores de servicios de intermediación que tomen medidas para impedir el envío a España de tales mensajes por un período de un año para las infracciones graves y seis meses para las leves.

Además la Ley plantea mecanismos ágiles para la resolución de conflictos, acorde con la realidad de la Sociedad de la Información. Es especialmente interesante la llamada acción de cesación[107] a la que se podrá recurrir cuando se incurra en actos contrarios a la *libertad informática* consistentes en el envío de comunicaciones comerciales no solicitadas siempre que lesionen *intereses colectivos o difusos de los consumidores*[108]. La acción de cesación puede

---

destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

[107] *art.30.2 de la LSSICE: la acción de cesación se dirige a obtener una sentencia que condene al demandado a cesar en la conducta contraria a la presente Ley y a prohibir su reiteración futura. Asimismo, la acción podrá ejercerse para prohibir la realización de una conducta cuando ésta haya finalizado al tiempo de ejercitar la acción, si existen indicios suficientes que hagan temer su reiteración de modo inminente.*

[108] art.30.1 de la LSSICE: *contra las conductas contrarias a la presente Ley que lesionen intereses colectivos o difusos de los consumidores podrá interponerse acción de cesación.*

definirse como aquella cuyo ejercicio pretende la paralización de una actividad empresarial ilícita y potencialmente perjudicial para los consumidores y que tiene por objeto la obtención de una sentencia mediante la cual no sólo se condene al demandado a cesar en una conducta contraria a la ley, sino también a abstenerse en lo sucesivo[109].

De acciones de cesación destinadas a la protección de los intereses colectivos de consumidores y usuarios existe una notable variedad. De hecho, la Directiva 98/27/CE relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, refiere hasta once supuestos contemplados en las directivas enumeradas en su anexo, entre los que destaca, la publicidad engañosa[110]. Cualquier persona física o jurídica aún sin resultar afectada, solamente llevada por un interés altruista podría ejercer la acción de cesación para la defensa de los intereses colectivos y difusos de los consumidores y usuarios[111].

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

Las sanciones previstas en la LSSICE referidas al spam son también aplicables cuando no se respeta el derecho de los abonados a no recibir llamadas

---

[109] Romero Jaime, D.J. Del charlatán al spam: publicidad molesta y libertad informática. Tutela judicial del consumidor y acciones de cesación, 2008.

[110] Directiva 84/450/CEE del Consejo, de 10 de septiembre de 1984, relativa a las aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de publicidad engañosa.

[111] art.31)a de la LSSICE

automáticas sin intervención humana o mensajes de fax con fines de venta directa sin consentirlas previamente.

Finalmente, la ley prevé para aquellos que realicen envíos publicitarios la habilitación de mecanismos sencillos y gratuitos a los que el abonado pueda dirigir su deseo de no recibir más mensajes publicitarios.

Por otro lado, como ya se ha visto, la Directiva 58/2002/CE sobre privacidad en las telecomunicaciones introdujo en el conjunto de la Unión Europea el sistema opt-in según el cual se requiere el consentimiento previo de la persona para el envío de comunicaciones con fines comerciales. De modo que cualquier envío con fines publicitarios quedará supeditado al consentimiento salvo que exista, tal y como recoge la LSSICE, una relación contractual previa y el destinatario no manifieste su voluntad en contra.

Actualmente la mencionada Directiva tiene su acomodo en la **Ley 32/2003 General de Telecomunicaciones,** en adelante LGT, que establece de modo similar a la LSSICE el principio de consentimiento previo que requiere éste para el envío de correo electrónico con fines comerciales salvo existencia de relación contractual previa. Si bien la citada Ley no recoge nada respecto a las llamadas no automáticas con fines de venta directa sí lo hace el artículo 69.2 del Real Decreto 424/2005[112] por el que se escoge las listas de exclusión como sistemas de regulación para este tipo de llamadas: *podrán efectuarse salvo las dirigidas a aquellos que hayan manifestado su deseo de no recibir dichas llamadas.*

Endurece el régimen de infracciones y sanciones previsto en la LSSICE en aquellos casos en los que se produzcan envíos masivos de spam, o remisiones a

[112] Por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

un mismo destinatario en el plazo de un año de más de tres comunicaciones no deseadas por medios electrónicos.

Finalmente, mientras la LSSICE establece que corresponde a la AEPD la imposición de sanciones en el caso de infracción por la remisión de comunicaciones comerciales no solicitadas efectuadas a través de correo electrónico o medios de comunicación electrónica equivalentes, la LGT concede la tutela de los derechos y garantías de abonados[113] y usuarios[114] en el ámbito de las comunicaciones electrónicas a la AEPD.

[113] Persona física o jurídica con contrato con el operador.

[114] Personas físicas o jurídicas que utilizan los servicios sin haberlos contratado.

Legislación comparada

En **España**, como hemos visto, se reguló por primera vez el fenómeno del spam en 2002 con la LSSICE una norma tan nueva como criticada por muchos sectores por ser bastante restrictiva en esta materia: establecía la prohibición absoluta al envío de comunicaciones comerciales no solicitadas a excepción de las consentidas por el destinatario. La ley resultaba contraria a la normativa de protección de datos y a la propuesta de Directiva sobre la privacidad de las comunicaciones electrónicas pues 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.

Varios expertos se preguntaron ya entonces cuánto tardaría en ser modificada, especialmente en lo relativo al spam, dado que la Directiva 2002/58/CE sobre la privacidad de las comunicaciones electrónicas aprobada sólo un día después de la ley española, el 12 de julio de 2002, regulaba el envío de comunicaciones electrónicas no solicitadas de manera no idéntica a como ésta lo hacía. Apenas un año ha bastado para que la nueva LGT haya modificado el núcleo del capítulo dedicado al spam.

La directiva reguló el envío de spam mediante el principio *opt-in* por el cual sólo se pueden enviar correos no solicitados a aquellos que expresamente lo han consentido. De este modo se distancia del principio *opt-out* que había regido la regulación anterior por medio del cual el remitente puede enviar correos electrónicos no solicitados a todos aquellos que previamente no se hayan

opuesto a su recepción en una apuesta clara por los derechos individuales por encima de la libertad de mercado[115].

No obstante se refiere únicamente a las comunicaciones comerciales enviadas por correo electrónico sin entrar a considerar otras formas publicitarias en Internet resultantes de la navegación a través de su estructura hipertextual como son los *banners* o las ventanas *pop-up* que también generan costes para el usuario en la medida que la navegación se ve ralentizada y el tiempo de conexión aumentado.

Por otro lado, la regulación del spam de la norma española antes de su modificación fue elogiada por asociaciones de usuarios informáticos como la Asociación de Usuarios de Internet (AUI) por suponer un primer paso para el control de esta plaga que afecta especialmente a internautas pero, al mismo tiempo, muy criticada por las asociaciones de empresas que operan en Internet por considerarse discriminados al no poder competir con el resto de empresas europeas por estar éstas sometidas a legislaciones con una regulación del spam menos restrictiva. Quizás por ello, la nueva LGT, ha modificado sustancialmente la materia del spam flexibilizando los requisitos para los correos no solicitados enviados por las empresas. Esta modificación incorpora una excepción que no existía en la anterior redacción sobre la prohibición del envío de comunicaciones comerciales no solicitadas sin consentimiento previo al posibilitarlas en el contexto de una relación contractual previa sobre los productos o servicios similares a los vendidos en aquélla. Es decir, la verdadera novedad permite a las empresas y profesionales, que ya tuvieron relación contractual con un cliente, enviarle información comercial mediante correo electrónico sin aviso o

[115] Plaza Soler, J.C., Los correos electrónicos comerciales no solicitados un año después de la LSSICE, 2004.

consentimiento previo. Se integra, por tanto, al ordenamiento jurídico español lo previsto en el ya mencionado artículo 13 de la Directiva 58/2002/CE.

El nuevo párrafo, no obstante, adolece de una imprecisión notable: la generalidad de la expresión productos similares a los que inicialmente fueron objeto de contratación con el cliente o la expresión relación contractual previa: similares en ¿qué?, ¿en precio?, ¿en estilo?[116], etc. En este punto la Directiva es algo más precisa al exigir que la dirección se obtenga en el contexto de la venta de un servicio o producto.

A diferencia de la redacción anterior, con la actual, una empresa que contrata con una persona y obtenga de ella sus datos de correo electrónico por una vía diferente a la del contrato pero lícita según la LOPD (de una guía de profesionales, por ejemplo) podrías enviarle correos electrónicos promocionales sin previo aviso sobre productos similares.

En opinión de Plaza Soler[117] se debería haber mantenido el requisito de que la dirección de correo electrónico se hubiera obtenido durante el procedimiento de contratación con un cliente. Asimismo la norma española obvia también hacer referencia a la finalidad de venta directa para la que la dirección de aquél con quien se mantuvo una relación contractual previa pueda ser utilizada.

Asimismo mientras que la LSSICE exige autorización previa y expresa, la Directiva, habla sólo de consentimiento previo. En lo referido a la obtención de los datos la norma española exige que los datos hayan sido obtenidos de forma lícita aunque sin precisar en qué momento, sin embargo, la Directiva exige además que hayan sido obtenidos en el contexto de la venta de un producto o servicio.

---

[116] Guillén Catalán, R. *Spam y comunicaciones comerciales no solicitadas*, 2005.

[117] Plaza Soler, J.C., Los correos electrónicos comerciales no solicitados un año después de la LSSICE, 2004.

El legislador español sigue sin mencionar si el destinatario de los mensajes de correo son sólo personas físicas o también jurídicas pese a que el apartado 5 del artículo 13 de la Directiva 2002/58/CE aconsejaba expresamente mencionarlo incluyendo así a las numerosas empresas que reciben miles de correos electrónicos no solicitados.

También la norma española obvia referenciar los 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 contenga una dirección válida, principios como veremos, importados de la legislación homóloga estadounidense. Tampoco contiene obligación alguna para que el prestador de servicios que recibe la notificación de un remitente trasladándole su no deseo de recibir comunicaciones comerciales le confirme que tal exclusión se ha producido.

El requisito de que no se disimule u oculte la verdadera identidad del remitente es especialmente importante a la hora de identificar la procedencia y fuente del spam y así poder ayudar a la autoridad competente sancionadora. Asimismo la obligación de situar al inicio del mensaje comercial no solicitado la palabra *publicidad* debe ser interpretada según explica el Ministerio de Ciencia y Tecnología como *en el asunto del mensaje*.

Por último, ni la directiva comunitaria ni la LSSICE prohíben explícitamente, como sí lo hacen las normas homólogas de algunos estados de EEUU, utilizar robots captadores de direcciones e-mail para enviar spam o comercializar programas de software que permitan enviarlo. Ni tampoco, para el caso español, se ha atribuido al envío de correos no solicitados con finalidad comercial la consideración de delito penal como sí lo ha hecho, por ejemplo, Italia.

Como veremos la adaptación de la directiva en el resto de países europeos ha sido muy dispar.

Así, en el **Reino Unido,** se excluye del derecho a no recibir mensajes no solicitados a las personas jurídicas o a los trabajadores de las mismas con dirección de correo corporativa. La dirección de correo electrónico debe obtenerse en el contexto de una venta o la negociación de la venta de un producto similar. Prevé el derecho del destinatario a no recibir correos comerciales pero no existe la obligación de identificar el mensaje publicitario como tal.

En **Austria** se prohíbe enviar, sin el consentimiento de sus destinatarios salvo que su dirección haya sido obtenida en el contexto de una venta y se use para anunciar productos similares siempre que se le permita oponerse en cualquier momento, correos comerciales no solicitados, SMS incluidos, si se envían a más de 50 destinatarios o si el contenido del correo tiene como finalidad el marketing. Se prohíbe enviar mensajes sin los datos de la persona por cuenta de quien se envían los mensajes o sin una dirección de respuesta válida.

En **Bélgica** la ley introduce el sistema *opt-in* y es el remitente del correo quien debe probar que el destinatario consintió su envío. El consentimiento no será necesario en el contexto de una relación contractual previa sobre productos o servicios similares. Asimismo el destinatario podrá oponerse en cualquier momento. Tampoco es necesario el consentimiento expreso para el envío de spam a personas jurídicas si las direcciones electrónicas de envío son de naturaleza impersonal (info@..., etc.).

Si el destinatario manifestase la voluntad de no recibir más correos publicitarios el remitente de tales correos debe enviarle una notificación reconociendo que ha recibido la petición, tomar las medidas necesarias para hacer cumplir la misma

así como llevar un listado actualizado de clientes que han decidido no recibir publicidad.

En **Dinamarca** se prohíbe el envío a quienes no hayan dado su consentimiento previo salvo que se haya dado voluntariamente la dirección de correo en el transcurso de una compra en Internet.

En **Italia** se permite el envío de correos no solicitados cuando el remitente anuncia productos de la misma naturaleza que el adquirido por el destinatario y obtenga sus datos en el contexto de la contratación del producto. Se garantiza el derecho de oposición por medio de procedimientos sencillos y gratuitos. Se sanciona el envío de mensajes sin que coste la identidad del emisor así como a ordenar al proveedor de acceso del emisor de los correos la implementación de filtros para evitarlos. Se castigan los envíos de spam hasta con 3 años de cárcel y 90.000 euros de multa situando de este modo a la legislación italiana como una de las más duras en Europa.

No obstante, en el plano internacional, el ordenamiento norteamericano tiene una enorme trascendencia porque además de ser la base para el resto de legislaciones de Internet es el que más ha desarrollado la regulación en materia de comercio electrónico.

El spam se ha regulado en varios estados norteamericanos. Conforme a la bibliografía consultada[118], 24 estados tienen normas de regulación de los correos electrónicos comerciales. La mayoría de los estados comparten las siguientes características en sus respectivas legislaciones:

- exigen que conste una palabra o unas siglas al principio del encabezamiento del mensaje

[118] Plaza Soler, J.C. La regulación de los correos electrónicos comerciales no solicitados en el derecho español, europeo y estadounidense, 2002

- obligan a que los correos contengan instrucciones para ejercitar las listas de exclusión de manera sencilla
- se prohíben los mensajes que contienen información falsa sobre la procedencia de los correos electrónicos o si no contienen una dirección válida y funcional del remitente. Se prohíbe la distribución de programas que permitan falsificar estas direcciones.
- no se permite la autorización del nombre de dominio de un tercero para enviar correo sin su consentimiento.
- algunos estados (Pennsylvania y Wisconsin) sólo regulan el envío de correo comercial no solicitado cuando contienen archivos o contenidos de naturaleza sexual. Quienes los envían están obligados a introducir palabras en el título del mensaje que los identifiquen como tales.

Respecto de la competencia territorial la mayoría de los estados declaran aplicables sus normas cuando el origen y el destino del correo comercial están dentro del mismo estado.

Nuevas iniciativas legislativas surgidas en EEUU desde el año 2002 manifiestan la toma de conciencia por la gravedad del problema del spam dada su posición de máximo emisor de spam circunstancia que socava la confianza del consumidor en las empresas americanas. Así se han visto aprobadas en 2003 varias iniciativas legislativas en el ámbito federal que afrontan muchos de los diversos problemas que se derivan del spam:

- La ley de protección de los teléfonos móviles contra el spam prohíbe el uso de la telefonía móvil para el envío de mensajes no solicitados.
- La ley para detener el marketing abusivo y sexual permitió la creación de un registro nacional de personas que no desean recibir correos electrónicos no deseados. Prohíbe los encabezamientos falsos en los

mensajes y obliga a incluir en el asunto del mensaje publicitario la abreviatura *ADV* para identificarlo como tal.

- La ley para reducir la distribución de spam exige que todos los correos comerciales se identifiquen como tales, una dirección real del emisor, encabezamientos que no induzcan a error e incluir instrucciones para darse de baja de la lista de destinatarios.
- La ley para reducir el spam presenta como novedad la diferencia entre correo masivo y no masivo considerando el primero el envío de más de un millar de mensajes en el plazo de dos días.
- La ley criminal del spam también distingue el correo masivo consistente en el envío de más de 100 mensajes en el plazo de 24 horas, 1.000 en el de 30 días o 10.000 en un año. Prohíbe el uso de equipos de terceros para enviar spam así como los encabezamientos falsos. También regula el uso de múltiples cuentas de correo o nombres de dominio para enviar mensajes.
- La ley de derechos de los propietarios de ordenadores obliga a la creación de un registro de personas que no deseen recibir correos comerciales.

Como observamos lo meritorio de estas iniciativas es la distinción por medio de número de envíos mínimos en un periodo de tiempo entre los verdaderos envíos masivos de correo comercial (el auténtico spam) y los mensajes comerciales no solicitados. Se observa el interés para que los remitentes de correo electrónico queden identificados así como para que aparezcan direcciones válidas de correo que permitan ejercitar la posibilidad de excluirse de las listas de correo. Sin excepción, todos los proyectos, adoptan el sistema de regulación *opt-out*, pretenden garantizar la transparencia de los envíos y establecen precauciones especiales cuando el contenido de los correos es sexual y va dirigido a menores.

Tras algunos años de vacilaciones en la legislación europea y norteamericana parece que en los últimos años se han clarificado las posiciones de ambos y mientras que en Europa se inclinan por el principio *opt-in*[119] para regular el envío no consentido de comunicaciones comerciales en EEUU han optado por el *opt-out* con restricciones, es decir, autoriza su envío a aquellos destinatarios que no se hayan opuesto a su recepción.

Esta diferencia evidencia que el tratamiento de los datos personales en uno y otro continente es bien diferente: así mientras que en EEUU los datos personales pueden ser objeto de tráfico económico y están protegidos por débiles regulaciones y la mayoría de las veces por códigos éticos de adhesión y cumplimiento voluntarios en Europa la Directiva 95/46/CE fue la primera norma al respeto y el origen de un acervo legislativo, más exigente y garantista, orientado a la protección de los datos de carácter personal a fin de evitar el tratamiento de éstos sin el consentimiento o conocimiento de sus titulares.

Dado que los EEUU son los principales emisores de spam y, sin embargo, se inclinaron por el sistema *opt-out* para regularlo, las airadas críticas procedentes de la Unión Europea pedían un cambio de normativa más exigente, acorde con las necesidades de un medio como Internet y las reclamaciones de los internautas con objeto de aproximarla más a la normativa europea. De hecho, el *Cam-Spam Act*[120] no sólo no ha disminuido el envío de spam sino que se ha visto aumentado de forma considerable y, en la mayoría de casos, los *spammers* incumplen con lo establecido en la norma.

---

[119] Según EuroCAUCE (coalición europea contra el correo comercial no solicitado) los países europeos cuya legislación recoge el principio *opt-in* son: Austria, Dinamarca, Finlandia, Alemania, Grecia, Hungría, Italia, Noruega, Polonia, Eslovenia y España. http://www.euro.cauce.org/es/countries/index.html [consultado el 05/08/2010]

[120] Ley de control de pornografía y mercadeo no solicitados, traducción de Controlling the Assault of Non-Solicited Pornography and Marketing Act.

Cuestiones deontológicas relacionadas

La difícil tarea de legislar en el medio Internet se debe a la ausencia de límites de carácter temporal, la aterritorialidad (opuesta al principio de territorialidad que acota la aplicabilidad de las legislaciones estatales y define la jurisdicción competente) y la globalidad que implica la deslocalización de las actuaciones y dificulta los intentos de regulación.

No obstante, hay juristas, entre ellos 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 puedan estar sujetos a diversos sistemas jurídicos nacionales al mismo tiempo*[121]".

Ante la dificultad de regular normativamente Internet por las razones expuestas anteriormente y con el fin de proporcionar seguridad jurídica a los sujetos en línea se recurre a la autorregulación como posible solución eficaz frente al pluralismo legal existente en la Red.

La autorregulación puede ser definida como la observancia de pautas de conducta cuyo cumplimiento se ha fijado previamente como objetivo. Supone, por tanto, la asunción, de quienes se someten al sistema de autorregulación, de observar y hacer cumplir las reglas establecidas a tal fin. Asimismo el sistema contempla la supervisión del cumplimiento efectivo de las normas, las auditorías periódicas para comprobar el grado de cumplimiento de las empresas adheridas, la creación de sistemas extrajudiciales de resolución de conflictos o la concesión de sellos de confianza que identifica a la empresa como adherida al sistema.

[121] Vázquez Ruano, T. La protección de los destinatarios de las comunicaciones comerciales electrónicas, 2008.

En un sistema autonormativo su cumplimiento solo posee fuerza vinculante para aquellos que previa y voluntariamente se han comprometido a cumplirlo. Su creación eficaz constituye un elemento esencial para limitar el flujo de contenidos no deseados, nocivos e ilícitos. La 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.

Dos son los mecanismos que conforman un sistema autonormativo o de autorregulación: los códigos de conducta o éticos, también llamados deontológicos y los sellos de confianza. Así, la elaboración de estos códigos supone el primer eslabón para la autorregulación. Se constituyen de pautas de comportamiento que establecen límites jurídicos en el marco electrónico y persiguen la adecuada tutela de intereses de las partes intervinientes. Asimismo establecen el órgano encargado de la supervisión y observancia de las pautas y de la resolución de las posibles controversias. Al estar sometidos al principio de legalidad no pueden contener pautas más flexibles ni contrarias a los preceptos mínimos contenidos en las normas. Finalmente en la media que son elaborados para generar confianza y seguridad en el usuario y consumidor de los servicios de la sociedad de la información éstos deben participar en su elaboración.

Por otro lado, 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"[122]. Dicho de otro modo, los sellos se identifican con la voluntad de aquellas empresas adheridas voluntariamente al desempeño de unas prácticas de conducta empresarial recogidas en el código ético.

Dada su importancia 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 la LSSICE.

La Directiva reconoce que los códigos de conducta a nivel comunitario constituyen un *instrumento privilegiado para determinar las normas deontológicas aplicables a la comunicación comercial*[123]. Asimismo *los Estados miembro fomentarán 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*[124].

La LSSICE promueve la elaboración de códigos de conducta al que considerar que son un instrumento especialmente válido para la adaptación de la normativa legal a las características específicas de cada sector al punto de obligar al prestador de servicios de la sociedad de la información a *disponer de los medios que permitan acceder por medios electrónicos de forma permanente, fácil,*

---

[122] Vázquez Ruano, T. La protección de los destinatarios de las comunicaciones comerciales electrónicas, 2008.

[123] considerando 32 de la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

[124] artículo 16 de la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

directa y gratuita a los códigos de conducta[125]. 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 versar 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 los sobre los cimientos extrajudiciales para la resolución de conflictos que surjan por la prestación de servicios de la sociedad de la información*[126].

Asimismo por su sencillez, rapidez y comodidad para los usuarios, se potencia igualmente el recurso al arbitraje y a los procedimientos alternativos de resolución de conflictos que puedan crearse mediante códigos de conducta para dirimir las disputas que puedan surgir en la contratación electrónica y en el uso de los demás servicios de la sociedad de la información[127].

En el campo publicitario 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 constituya un instrumento útil en el proceso económico respete los derechos de los consumidores y la lealtad competencial.

Así, en la autorregulación publicitaria española, hay que destacar la labor realizada por la Asociación para el Autocontrol de la Comunicación Comercial. En

[125] artículo 10.g de la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico

[126] artículos 18.1 y 18.3 de la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico

[127] artículo 32 de la Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico

el ámbito de la publicidad en Internet estableció en 1999 el Código Ético de Publicidad en Internet. En 2002 se integró 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** y así abarcar tanto las comunicaciones comerciales como los aspectos contractuales de las transacciones comerciales con consumidores realizadas a través de Internet y otros medios electrónicos, sin olvidar la necesaria protección de datos personales tanto en las comunicaciones comerciales como en la contratación electrónica con consumidores.

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 de electrónicos de comunicación a distancia por personas físicas o jurídicas con establecimiento permanente en España o dirigido de forma específica al mercado español*[128].

La regulación que establece 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 de publicidad cubre no sólo su resolución a nivel nacional sino también cubre las la resolución de controversias transfronterizas a nivel comunitario. El control del cumplimiento del código corresponde a dos órganos extrajudiciales y sus resoluciones son de obligado cumplimiento para las empresas adheridas al código. Por un lado, el Jurado de la Asociación para el Autocontrol de la Comunicación Comercial es el encargado de resolver las reclamaciones en materia de publicidad por otro, la Junta Arbitral Nacional de Consumo resuelve las reclamaciones en materia de contratación

[128] artículo 2 del Código Ético de Comercio Electrónico y Publicidad Interactiva

electrónica no resueltas por la por mediación de la Asociación Española de Comercio Electrónico.

Así, en el primer grupo de normas generales, se establece que la publicidad en medios electrónicos deberá ser decente, honesta y veraz. Deberá cumplir el principio de identificación de la publicidad en cuanto a tal y el principio de identificación del anunciante (del mismo modo que establecen las distintas normativas comunitarias y nacionales para las comunicaciones comerciales electrónicas[129]), el principio de información en cuanto a información general, coste o precio de acceso al mensaje publicitario y la identificación clara de las ofertas promocionales, obtención de datos personales y, por último, el principio de respeto de los derechos de propiedad intelectual o industrial y el de lealtad con los competidores.

El segundo grupo de normas especiales se aplica a las distintas formas publicitarias en línea. De este modo tenemos que la publicidad enviada mediante mensajes de correo electrónico u otros medios de comunicación individual equivalentes[130], que en todo caso deberá identificarse claramente como tal, no se admitirá si no ha sido autorizada o solicitada expresamente por el destinatario.

---

[129] Directiva 2002/58/CE sobre la privacidad y las comunicaciones comerciales: **artículo 13.4** prohíbe en cualquier caso la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule u oculte la identidad del remitente. Directiva 2000/31/CE sobre el comercio electrónico: **considerando 30** de la establece que las comunicaciones comerciales no solicitadas han de ser en todos los casos claramente identificables como tales, el **artículo 6** establece la información exigida para las comunicaciones comerciales, entre otra, la identificación clara tanto de la comunicación como de la persona física o jurídica en nombre de la cual se hagan.
LSSI: **artículo 20,** establece la información exigida a las comunicaciones comerciales por vía electrónica, entre otra, deberán ser claramente identificables como tales y deberán indicar la persona física o jurídica en nombre de la cual se realizan.

[130] artículo 9 del Código Ético de Comercio Electrónico y Publicidad Interactiva.

El código apuesta por el consentimiento regulado por el sistema opt-in o de listas de inclusión voluntarias, no obstante, son admisibles cualesquiera que garanticen la prestación del consentimiento. De igual modo se deberá informar con claridad al destinatario sobre la opción de no recibir publicidad y proporcionarle un mecanismo sencillo para la revocación del consentimiento.

Por otro lado la publicidad difundida a través de grupos de noticias, chats, foros y similares[131] no se autoriza sin el consentimiento previo del moderador del punto de encuentro, o en su defecto, del proveedor de servicios o sin que se ajuste a las reglas de admisión de publicidad establecidas en esos grupos, foros, etc. Tampoco la publicidad en la World Wide Web[132] podrá impedir la libre o normal navegación del usuario y deberán permitir que pueda salir con facilidad del mensaje publicitario o eliminarlo.

Por último, otra de las cuestiones deontológicas relacionadas recogidas en el código es la protección de datos personales. En él se establece 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[133]. Asimismo prohíbe la recogida 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

[131] artículo 10 del Código Ético de Comercio Electrónico y Publicidad Interactiva.

[132] artículo 11 del Código Ético de Comercio Electrónico y Publicidad Interactiva.

[133] artículo 20 del Código Ético de Comercio Electrónico y Publicidad Interactiva.

como de los derechos de acceso, rectificación, cancelación y oposición[134]. Asimismo las empresas proveerán a los usuarios de información clara y comprensible sobre la presencia y finalidad de las *cookies*[135] u otros dispositivos o técnicas similares así como de cuándo queda imposibilitado el acceso a un recurso o servicio por ser necesario el envío e instalación de cookies.

A pesar de las ventajas que para la regulación del envío de spam puede tener la autorregulación, los autores contrarios al sistema de autorregulación, afirman que por ser las propias entidades empresariales las que apuestan por la autorregulación es lógico pensar que apuesten más por sus intereses que por los de los usuarios y consumidores.

[134] artículo 21 del Código Ético de Comercio Electrónico y Publicidad Interactiva.

[135] artículo 24.1 del Código Ético de Comercio Electrónico y Publicidad Interactiva: las cookies son pequeños ficheros de datos enviados por los servidores web a los programas navegadores de los usuarios y que guardados en un directorio específico reúnen información.

Elaboración de una guía para el cumplimiento de la legislación española y europea respecto del spam

La legislación podrá disuadir e impedir el envío de spam pero no es suficiente por sí sola. El objetivo, por tanto, es conseguir que la prohibición del spam tenga la máxima eficacia y dotar de acciones tendentes a reducir su volumen. Para lo cual las acciones contempladas en la guía, que tienen su base en la Comunicación de la Comisión Europea sobre las comunicaciones comerciales no solicitadas[136], se centran en el cumplimiento efectivo de la legislación en torno al régimen de consentimiento previo por los estados miembros y las autoridades públicas, en la autorregulación por parte de la industria, en las soluciones técnicas, en la sensibilización de los consumidores, en la cooperación internacional, en la represión del incumplimiento, en la investigación y desarrollo tecnológicos y el recurso a la E-justicia.

Sólo podrá frenarse la proliferación de spam si todos los interesados, desde los estados miembros y las autoridades públicas hasta los consumidores y usuarios de Internet y las comunicaciones electrónicas y las empresas desempeñan el papel que les corresponde.

La aplicación del régimen de consentimiento previo debe ser prioritaria en todos los estados miembros. Éste incluye tres normas fundamentales:

1. el envío de mensajes electrónicos con fines comerciales se supedita al consentimiento previo de los abonados[137]. Se prevé una excepción limitada para

[136] 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.

[137] la persona física o jurídica que sea parte en un contrato con el proveedor en un servicio público de telecomunicaciones para la prestación de tales servicios. En Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

los mensajes de correo electrónico o SMS o MMS enviados por una empresa a clientes con relación contractual previa siempre que versen sobre productos o servicios similares a los que dio origen a la primera contratación. Éste régimen se aplica a los abonados que son personas físicas pero los estados miembros pueden hacerlo extensible a las personas jurídicas.

2. es ilícito disimular u ocultar la identidad del remitente por cuenta de quien efectúa la remisión.

3. todos los mensajes electrónicos deben mencionar una dirección de respuesta válida donde el abonado pueda pedir que no se le envíen más mensajes.

El medio más eficaz para hacer cumplir el régimen de consentimiento previo lo constituye un enfoque equilibrado que incluya el cumplimiento de la legislación, la imposición de normas, y la autorregulación. Con el fin de evaluar el funcionamiento práctico del sistema de consentimiento previo y de establecer medidas adecuadas a problemas concretos es necesario obtener información objetiva y actualizada en torno a las tendencias en materia de spam, las denuncias de los usuarios y las dificultades de los proveedores de servicios de Internet y correo electrónico. Esta información puede ser obtenida a través de las acciones enumeradas a continuación y que podrían servir de guía para el cumplimiento de la legislación española y europea en la lucha contra el spam.

Las siguientes acciones junto a sus iniciativas constituyen una posible solución para el cumplimiento efectivo de la legislación sobre el spam y su probable control.

- **ACCIONES DE APLICACIÓN Y DE CUMPLIMIENTO DIRIGIDAS PRINCIPALMENTE A LOS GOBIERNOS Y LAS AUTORIDADES PÚBLICAS**

  Es necesario crear unos mecanismos que garanticen el cumplimiento de la normativa así como la evaluación de su eficacia y su seguimiento en el ámbito

de los recursos y sanciones, mecanismos de denuncia y cooperación internacional.

a. **recursos y sanciones**: las sanciones administrativas parecen ser más adecuadas que los recursos judiciales al problema del spam. Tienen menor coste y su gestión es más ágil. Así las cosas, un inconveniente que presenta la aplicación de las normas que regulan el envío de spam ha sido la variada incorporación que ha tenido en sus respectivos acervos legislativos por parte de los estados miembros. No todos los gobiernos designan la misma autoridad pública como responsable de hacer cumplir la normativa. No todos los gobiernos imponen las mismas sanciones ante una misma infracción. Recordemos que la naturaleza peculiar del spam y su medio electrónico pueden afectar a distintos derechos reconocidos en diversas leyes estatales y su aplicación en ocasiones puede llegar a ser difusa, tales como el derecho a la intimidad, la privacidad, la protección de datos de carácter personal, etc.

No todas las autoridades responsables pueden actuar contra las personas físicas ni tampoco tienen la posibilidad de imponer sanciones. Las denuncias en función del país desembocan o no en una investigación y los actores encargados de iniciar la misma tampoco son los mismos. No todos los estados prevén vías de recursos y multas en su derecho administrativo o penal. Incluso aunque se establece una distinción entre sanciones leves y graves éstas varían mucho de un estado a otro. En unos países es el propio consumidor en otros, en cambio, los mecanismos de denuncia están contemplados en el ámbito de la autorregulación.

Una solución pasaría por la armonización legislativa de los estados miembros en la tipificación de delitos y regulación de los procedimientos jurídicos aplicables teniendo en cuenta que se trata de un problema común a todos los

estados y persigue una misma finalidad, a saber, eliminar las dificultades que merman la confianza de los consumidores en un entorno telemático. En este sentido, la sanción administrativa constituye un procedimiento rápido, eficaz y asequible para hacer aplicar el régimen de consentimiento previo y establecer posibilidades adecuadas para que las víctimas reclamen daños y perjuicios.

Por otro lado, las medidas represivas están sujetas a importantes diferencias entre los estados miembros en lo referido al número de denuncias objeto de persecución. Así mientras algunas autoridades nacionales no han dudado en iniciar un número sustancial de investigaciones en otros estados este número ha sido muy limitado.

b. **denuncias**: una aplicación eficaz de las normas implica contar con unos mecanismos de denuncia adecuados que puedan ser usados por los afectados sin grandes esfuerzos. En este sentido la implantación de **buzones electrónicos,** también llamados buzones spam, a los que los destinatarios de spam puedan enviar las denuncias y los mismos correos no solicitados, constituye un recurso de gran valor informativo. Por un lado es una práctica sencilla y nada costosa que debe alentar (y parece hacerlo) a los usurarios a denunciar infracciones y contribuir a que la legislación se aplique de modo más eficaz. Por otro lado proporciona información de gran interés en el seguimiento y la medición de la amplitud y el alcance del spam. Estos buzones deben permitir investigaciones y análisis destinados a comprender mejor el problema y fijar prioridades en materia de cumplimiento de la normativa.

Especial interés por su relevancia cobra el tratamiento eficaz de las **denuncias transfronterizas** de modo que las denuncias formuladas por usuarios de un estado miembro referidas a mensajes no solicitados recibidos

de otro estado miembro puedan ser atendidas eficazmente. Para ello se hace indispensable la cooperación y el intercambio de información entre las autoridades nacionales responsables de la protección de datos, de los consumidores y de la reglamentación de las comunicaciones electrónicas a fin de evitar el solapamiento de competencias y la duplicidad de funciones entre las distintas autoridades. 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[138].

c. **cooperación internacional**: dado el carácter transfronterizo del spam se requiere una sólida cooperación cuya finalidad persiga hacer extensible el régimen de consentimiento previo aplicable a las comunicaciones comerciales no solicitadas con destino u origen en redes de telecomunicación sitas en la Unión Europea al resto de comunicaciones procedentes de terceros países. Su aplicación es más complicada pero conseguirlo es vital dado que gran parte del spam procede del exterior de la Unión Europea. Serán, por tanto, objetivos de la cooperación internacional promover la aprobación de una legislación adecuada en los terceros países, garantizar la aplicación real de las normas aprobadas e impulsar la cooperación con el sector privado, principalmente con proveedores de servicios de Internet y proveedores de servicios de correo electrónico para localizar a los remitentes de spam.

La participación activa en foros destinados a la lucha antispam promovidos por organismos como la Organización de Cooperación y Desarrollo Económicos[139] (OCDE), la Unión Internacional de Telecomunicaciones[140], las

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

[139] Foro que tiene por objetivo la coordinación de la lucha contra la práctica del spam y la obtención de una respuesta internacional en las diversas políticas. Entre sus objetivos

Naciones Unidas[141] o los acuerdos suscritos[142] y los encuentros iberoamericanos[143] ponen de manifiesto el interés por enfrentarse al spam desde una perspectiva plural e internacional.

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

– la creación de la red de contacto de las autoridades responsables en materia de spam cuya misión es 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.
– el plan de acción de Londres cuyo objetivo básico es el establecimiento de un procedimiento de cooperación transfronterizo a nivel mundial por medio de la reagrupación de 20 autoridades de los países encargados del seguimiento de la aplicación de la legislación que regula el envío de comunicaciones comerciales no solicitadas.

---

destacan: el estudio de la evolución de la práctica del spam y de la eficacia de las medidas adoptadas, la promoción de la cooperación entre las autoridades competentes en los procedimientos de solicitud de ayuda e investigación, el establecimiento de medidas técnicas antispam o la educación en usuarios sobre los riegos de Internet y las comunicaciones electrónicas. Adoptó en abril de 2006 una recomendación sobre cooperación transfronteriza para dar cumplimiento a la legislación sobre el spam en la se urgía a las autoridades responsables a compartir información y colaborar.

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

[141] Declaración de la Cumbre Mundial sobre la Sociedad de la Información (Ginebra. 2003)

[142] En el caso español 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.

[143] Encuentro Iberoamericano (3er. Cartagena de Indias. 2004) Declaración de Cartagena de Indias con ocasión de la celebración del III Encuentro Iberoamericano de protección de datos.

– la cooperación entre la UE y EEUU, Canadá, China y Japón, principalmente, en el ámbito de la lucha contra los contenidos no deseados, nocivos e ilícitos.

Para la consecución de esta cooperación internacional, en el caso español, la AEPD ha firmado varios documentos de colaboración y asistencia recíprocas con las instituciones encargadas tanto a nivel comunitario como extracomunitario:

– **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. Desde este grupo se ha acordado la creación de un marco intraeuropeo para el intercambio de información sobre denuncias de spam indicando qué hacer cuando se reciben estas denuncias. El punto común de estos países es el artículo 13 de la Directiva 2002/58/CE. En virtud de este acuerdo, al recibir una queja internacional, antes de remitirla a la autoridad nacional competente se ha de verificar que la denuncia es viable y que es remitida por una persona física. También se ha de informar a ésta que sus datos personales serán cedidos a otra autoridad. Deberán también mantener el secreto de las informaciones y denuncias.

– **Relaciones con Estados Unidos**

Hay que tener en cuenta que la lucha contra el spam en los EEUU parte de una normativa muy distinta a la europea. En EEUU se establece un sistema opt-out que a diferencia del opt-in no requiere consentimiento previo sino que autoriza el envío de comunicaciones comerciales mientras que el destinatario no manifieste su oposición a recibirlas. Pues bien, con esta idea de

cooperación global firmó la agencia española de protección de datos en 2004 un convenio con la Comisión Federal del Comercio de EEUU un acuerdo de cooperación administrativa para luchar contra el spam. En virtud del acuerdo ambas partes se comprometen a facilitar la formación de usuarios y empresas en relación con el spam, promover códigos de conducta de buenas prácticas, intercambiar información sobre soluciones técnicas avanzadas y mantenerse informados sobre las novedades, colaborar con las universidades de los respectivos países para promover la investigación, conferencias y cursos sobre la materia así como prestarse asistencia mutua en sus investigaciones.

– **Relaciones multilaterales**

Dan lugar al ya mencionado plan de actuación conjunta (London Action Plan) cuyo objetivo, entre otros, es el desarrollo de contactos internacionales para la investigación de casos de spam. A tal fin los suscriptores del plan de acción asumen impulsar la comunicación entre ellos y así supervisar de manera más eficiente el cumplimiento de la normativa, organizar conferencias periódicas para el debate y exposición de asuntos relacionados con el spam o favorecer el diálogo entre organismos públicos e industria para la actuación conjunta y cooperativa.

– **Relaciones con Iberoamérica**

La AEPD en su intento por fijar posiciones comunes sobre protección de datos personales en los países iberoamericanos participó en el año 2004 en el III Encuentro Iberoamericano donde fueron abordados temas como el ataque a la privacidad en el sector de las comunicaciones electrónicas e Internet así como la lucha anti-spam. Se acordó fijar medidas técnicas y legislativas para evitar el spam, promover la colaboración internacional o favorecer iniciativas

de autorregulación del sector de las comunicaciones electrónicas que complementen el marco regulador.

– **Foros internacionales**

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

El Foro Abuses[144] es una iniciativa que reúne a algunas de las organizaciones profesionales que tienen que trabajar diariamente para evitar los impactos y las amenazas sobre los sistemas de información. Sus objetivos principales están relacionados con la lucha contra los abusos informáticos como son el correo no deseado, los códigos maliciosos, los ataques a sistemas informáticos o las violaciones de derechos de propiedad intelectual. Las organizaciones participantes del foro intercambian información sobre la procedencia de los ataques, los medios utilizados y, en general, todos los datos que puedan resultar útiles para combatir cada ataque. De este modo, colaboran para eliminar las amenazas lo antes posible y minimizar su impacto. El foro, participado por empresas privadas, ha sido promocionado a través de la red de información RedIris. La cooperación de este foro se produce también a escala europea a través de E-COAT (European Cooperation of Abuse Fighting Teams dado que el problema de la seguridad de las redes repercute a nivel global.

[144] http://www.rediris.es/abuses

- **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. El Espacio Europeo de Justicia (EEJ) responde a este objetivo y surge a partir de la entrada en vigor del Tratado de Ámsterdam. Su objetivo es el establecimiento de un conjunto de instrumentos legislativos destinados a garantizar el reconocimiento mutuo de las decisiones judiciales y la cooperación entre autoridades judiciales nacionales.

Uno de los principales retos para la construcción del EEJ es establecer los instrumentos que permitan mejorar la eficacia práctica de los instrumentos jurídicos adoptados. Si la administración electrónica responde al deseo de facilitar y agilitar los procedimientos administrativos por medio de las TIC, bajo el neologismo e-justicia, situamos el recurso a las TIC para mejorar el acceso de los ciudadanos a la justicia y la eficacia de la acción judicial entendida como toda actividad orientada a la resolución de litigios. La mejora del acceso a la información tiene en la creación del portal e-Justicia su principal referente. Entendido como una plataforma de información tendrá como finalidad orientar e informar al ciudadano europeo en su lengua de los sistemas de redes judiciales, los procedimientos judiciales y los instrumentos creados en materia judicial a fin de evitar que éste no pueda defender sus derechos en otros países miembros de la UE debido al desconocimiento de las normas vigentes. Por tanto, proporcionará al ciudadano, entre otra, información europea y nacional sobre los derechos de las víctimas en el procedimiento penal y las indemnizaciones, los derechos fundamentales que tienen los ciudadanos de cada estado miembro y los principios fundamentales relacionados con el recurso del ciudadano a una jurisdicción de otro estado miembro o a la defensa ante dicha jurisdicción.

Entre las propuestas y recomendaciones dirigidas a los órganos judiciales y los cuerpos y fuerzas de seguridad de los estados miembros los expertos señalan las siguientes:

- favorecer y estimular de forma activa la formación de continua de jueces y fiscales sobre este tipo de delitos.
- cooperación entre los jueces y los cuerpos y fuerzas de seguridad del estado a fin de intercambiar información.
- autoridad para requerir información relativa a las direcciones IP a los operadores de forma preventiva cuando haya sospechas fundadas de actuaciones ilícitas.
- disponer de recursos suficientes para detectar a los remitentes de spam activos en la UE o fuera de ella y que ocultan su identidad sirviéndose de la de otros usuarios.

- **ACCIONES TÉCNICAS Y DE AUTORREGULACIÓN PARA LA INDUSTRIA**

La industria, representada por los proveedores de servicios de Internet, debe desempeñar una labor indispensable en la lucha contra el spam. Dado que toda la normativa desarrollada tiene en el mercado y en la economía su razón de ser puede y debe desempeñar un papel decisivo al convertir el régimen de consentimiento previo en una práctica comercial cotidiana. De ser así y, en el caso de los contratos suscritos con proveedores de Internet y de correo electrónico, éstos podrían contribuir a la lucha contra el spam si incorporasen en sus cláusulas la obligación de no utilizar sus servicios para el envío de spam y establecer sanciones en caso de incumplimiento. Asimismo la adopción de una política de filtrado más firme y voluntariosa que facilitase información suficiente sobre los filtros antispam y su implementación gratuita haría más creíble su interés por frenar el avance de spam.

Como ya se ha indicado estas acciones incluyen medidas que conciernen principalmente a los agentes del mercado en el ámbito de la autorregulación y la solución técnica. Entre las primeras se encuentran la adaptación de las disposiciones contractuales a las nuevas regulaciones normativas, la elaboración y difusión de códigos de conducta[145] o de buenas prácticas adecuados al régimen de consentimiento previo, el fomento de prácticas de comercialización aceptables y la utilización de sellos de confianza para indicar el respeto al sistema de consentimiento previo y el sometimiento a los códigos de buenas prácticas.

La solución extrajudicial de litigios queda recogida en el artículo 17 de la Directiva sobre el comercio electrónico[146]. Para el caso que nos ocupa, comunicaciones comerciales no solicitadas, la solución extrajudicial de conflictos podría resultar especialmente útil y podría contribuir a un mayor respeto de las nuevas normas. Su instauración exige la cooperación entre las autoridades y la industria.

Las soluciones técnicas pasan por la adopción de medidas de seguridad para los servidores y el desarrollo de sistemas de filtrado antispam. Sin embargo no todas las técnicas de filtrado ofrecen las mismas garantías en materia de protección de datos e intimidad. Además pueden plantear problemas de eficacia si los sistemas llegan a bloquear el correo electrónico útil (falsos positivos) o dejan pasar el

[145] Los códigos de conducta se recogen en el artículo 16 de la Directiva sobre el comercio electrónico. Su enunciado establece para los Estados miembros y la Comisión el fomento la elaboración de los códigos de conducta a nivel comunitario a través de asociaciones y organizaciones comerciales, profesionales o de consumidores en cuya redacción participarán y la posibilidad de acceder a ellos vía electrónica y mención específica a los códigos en materia de protección a menores y dignidad humana y a las asociaciones que representen a colectivos de discapacitados e invidentes.

[146] Los Estados miembros velarán porque la legislación en caso de desacuerdo no obstaculice el uso de mecanismos de solución extrajudicial, alentarán a los órganos responsables a proporcionar garantías en los procedimientos e incitarán de igual modo a que informen a la Comisión de la Unión Europea de las decisiones que adopten en torno a la resolución del conflicto y que tenga especial relevancia para la Sociedad de la Información y en concreto sobre prácticas, usos o costumbres relacionados con el correo electrónico.

spam (falsos negativos) u otro tipo de problemas como los relacionados entre el filtrado y la libertad de expresión o la obligación contractual que tienen los proveedores de servicios de Internet y correo electrónico de transmitir mensajes de correo a sus abonados.

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

Las recomendaciones y propuestas de los expertos dirigidas a los fabricantes y proveedores de servicios de informática son, entre otras:

– mejorar las actuaciones por parte de los operadores para orientar las medidas de seguridad al bloqueo de determinados servicios como el bloqueo del correo de salida fácilmente monitorizable a través de un filtro para aquellas máquinas cuya IP se identifique asociada a un uso malicioso del servicio de correo por medio del envío de spam, malware y troyanos o un control en el acceso a aquellas máquinas que alojan sitios fraudulentos.

– aplicar políticas avanzadas de gestión de correo electrónico y proporcionar un servicio de salida de correo electrónico cortado por defecto y obligar a que el envío de ese correo se valide por el servidor del proveedor ISP donde se puede instaurar un mayor control del flujo de comunicaciones con restricciones y medidas de seguridad contra el mal uso del correo electrónico. En este sentido Google acaba de lanzar una nueva herramienta para facilitar la clasificación de los e-mails en su servicio de correo electrónico Gmail. Se trata de *Priority Inbox* una aplicación que clasificará cada nuevo correo en función de su importancia de modo que atendiendo a parámetros como la

asiduidad con la que se reciben correos, los usuarios con los que se chatea y la procedencia de los correos que se abren y responden de los que no ponderará los correos en tres categorías: *importante y no leído*, *marcado* y *todo lo demás*.

Por otro lado la Comisión Europea insta a las empresas a adaptar las prácticas de venta directa, las prácticas contractuales y los códigos de buenas prácticas a la normativa de protección de datos y al régimen de consentimiento previo. En el caso de proveedores de servicios se les insta a aplicar una política de filtrado del correo electrónico que se ajuste a las recomendaciones, especialmente, las emitidas por el grupo de trabajo sobre la protección de datos.

- **ACCIONES DE SENSIBILIZACIÓN DIRIGIDAS PRINCIPALMENTE A CONSUMIDORES Y USUARIOS DE LAS TELECOMUNICACIONES**

Incluye propuestas en ámbitos como la prevención, la educación y el papel que deben adoptar los gobiernos, las autoridades públicas, los agentes del mercado y las asociaciones de consumidores frente a la notificación de denuncias relacionadas con el envío de spam.

La acción más pertinente es el desarrollo de campañas de información orientadas a distintos grupos y realizadas por distintos canales (no únicamente a través de la Red) donde se den a conocer explicaciones básicas pero globales sobre las nuevas normas y los derechos de las empresas y los consumidores.

Concretamente información práctica sobre:

– las prácticas de comercialización aceptables ajustadas al régimen de consentimiento previo, clarificando el concepto de recogida legítima de datos personales.
– cómo evitar el spam incluyendo servicios y productos disponibles (sistemas de filtrado).

– medidas en caso de recibir el spam: a quién dirigir y cómo notificar las denuncias, o si existen, dar a conocer los mecanismos de solución extrajudicial de conflictos.
– los riesgos que implica la comunicación de datos personales en Internet.
– las asociaciones de usuarios activas en este campo.

Otras medidas de sensibilización

Los estados miembros han invertido en campañas de sensibilización dirigidas a los usuarios y consumidores freten al spam y en medios para limitar su envío. Los proveedores de servicios de Internet ofrecen a tal fin a sus abonados consejos sobre la forma de protegerse contra los programas espía y los virus.

El programa **Safer Internet** constituye, a nivel comunitario, la toma de conciencia del spam al estar explícitamente concebido para combatir, entre otros, las comunicaciones electrónicas no solicitadas. El objetivo general[147] es promover un entorno favorable al desarrollo de la industria relacionada con Internet mediante el fomento de un uso seguro de la Red y la lucha contra los contenidos ilícitos[148] y nocivos[149]. El programa se articula en torno a tres ejes:

– implantación de una red europea de líneas directas llamadas *hotlines* que permiten a los ciudadanos denunciar los contenidos ilícitos y nocivos que circulan por Internet, trasmitir la denuncia a la instancia pertinente (policía, proveedor de servicios de Internet o de correo electrónico) y configurar de

[147] http://europa.eu/legislation_summaries/information_society/l24190_es.htm [consultado el 25/06/2010)

[148] De su contenido debe ocuparse desde el principio las autoridades policiales y judiciales. La industria puede ayudar significativamente para limitar su circulación por medio del establecimiento de mecanismos eficaces de autorregulación.

[149] Debe dar la posibilidad a los usuarios de rechazarlos dado que pueden ser contenidos autorizados pero con distribución restringida (sólo para adultos) o sin restringir pero con contenidos que sujetos a la libertad de expresión puedan sin embargo ofender a determinados colectivos o individuos.

este modo una Red más segura. En este sentido un sistema de autorregulación es factor esencial para limitar el flujo de spam y contenidos ilícitos y nocivos. A tal fin se crea el foro *Una Internet más segura* cuyo objetivo es el intercambio de experiencias e información en el ámbito de la autorregulación: temas en torno a la evaluación de la calidad de sitios web, la calificación de contenidos, la adopción de códigos de conducta o el establecimiento de vínculos a organismos de autorregulación no europeos.

– desarrollo de sistemas de filtrado anti spam y clasificación cuyo objetivo sea dotar a los responsables de menores seleccionar contenidos que sean adecuados.

– iniciativas de sensibilización orientadas a informar sobre la manera más adecuada de proteger a los menores contra la exposición a contenidos que podrían ser inadecuados en su educación así como sobre los problemas de seguridad relacionados con el uso de Internet. Asimismo deben abordar las categorías de contenidos, a saber, ilícitos, nocivos y no deseados, implicados en cuestiones relacionadas tales como la protección de los consumidores, la protección de datos y la seguridad de la información y las redes.

La continuidad del programa se denomina **Safer Internet Plus**[150] y tiene como finalidad garantizar una cobertura y cooperación de alcance europeo e incrementar la eficacia a través del intercambio de información y fomentar un uso más seguro de Internet y el resto de tecnologías en línea especialmente en niños.

El nuevo programa se orienta a la inversión en hotlines y en medidas tecnológicas que permitan a los usuarios limitar la cantidad de contenidos no

[150] http://europa.eu/legislation_summaries/information_society/l24190b_es.htm [consultado el 28/06/2010]

deseados y perjudiciales y gestionarlos. La inversión en hotlines incluye la creación de líneas directas nacionales con capacidad de interactuar y cooperar con otros centros de la red europea de líneas directas, la recogida de datos cualitativos sobre su establecimiento y funcionamiento, la aceleración de su implementación y finalmente la implantación de un nodo coordinador de la red que aumente la capacidad operativa y favorezca los intercambios de información y experiencias.

La inversión en medidas tecnológicas incluye la evaluación de la eficacia de los filtros disponibles, la adopción de sistemas de clasificación de contenidos y etiquetas de calidad, el acceso a sistemas de filtrado en lenguas no cubiertas por la industria de las tecnologías emergentes.

En la misma línea la **Agenda de Túnez,** adoptada a finales de 2005 por la Cumbre Mundial de la Sociedad de la Información, subraya que la seguridad de Internet es uno de los ámbitos en los que resulta necesario mejorar la cooperación internacional y aborda en su punto 41 la problemática del spam: "exhortamos a todas las partes interesadas a que adopten un enfoque multidimensional para contrarrestar el correo basura que incluya la educación del consumidor y de las empresas así como el establecimiento tanto de una legislación adecuada como de los mecanismos y organismos necesarios para su aplicación, el perfeccionamiento permanente de las medidas técnicas y autorreguladoras, las prácticas idóneas y la cooperación internacional"[151].

[151] http://www.itu.int/wsis/doc2/tunis/off/6rev1.doc [consultado el 12/07/2010]

- **INVESTIGACIÓN Y DESARROLLO TECNOLÓGICOS**

Conscientes los organismos de la Unión Europea y la industria de la importancia del desarrollo científico y tecnológico aúnan esfuerzos con vistas a la creación de un Espacio Europeo de Investigación.

A tal fin los programas marco de investigación y desarrollo tecnológico impulsados por la Comisión Europea constituyen marcos generales de las actividades de la UE en el ámbito de la ciencia, la investigación y la innovación. Concretamente, el **sexto programa marco** (2002-2006)[152], constituye el principal instrumento legal y financiero de la UE para aplicar el Espacio Europeo de Investigación. Entre sus programas, los proyectos específicos para ayudar a frenar el spam y luchar contra otras formas de programas maliciosos, centran sus actividades de investigación, entre otras, en los estudios sobre tecnologías que velan por la seguridad y la confidencialidad de los sistemas informáticos así como por los derechos y la vida privada de los ciudadanos[153]. Entre las medidas acometidas en este campo figuran la creación de una comunidad científica especializada en el control de los programas maliciosos, la puesta a punto de una infraestructura europea para controlar el tráfico a través de Internet y la elaboración de filtros adaptables contra el *phishing* que permitan detectar amenazas desconocidas y ciberataques.

Por último, uno de los programas del séptimo programa marco de investigación para el periodo 2007-2013, concretamente el de Cooperación, incluye en sus campos temáticos uno, la seguridad y el espacio, que sirve para dar continuidad

[152] http://europa.eu/legislation_summaries/food_safety/general_provisions/i23012_es.htm [consultado el 29/06/2010]

[153] Sexto Programa Marco (2000-2006): Tecnologías para la sociedad de la información http://europa.eu/legislation_summaries/information_society/i23014_es.htm [consultada el 29/06/2010]

a la línea de estudio de nuevas medidas para garantizar la seguridad de las redes información.

Con todo, los factores que parecen influir sobre la eficacia de los mecanismos de aplicación son:

- algunas autoridades reguladoras carecen todavía de poderes coercitivos y por tanto de la posibilidad de hacer cumplir la legislación por medio de multas o sanciones.
- la naturaleza y los mecanismos de denuncia y los recursos a disposición de particulares y empresas.
- la necesidad de claridad y coordinación entre las autoridades nacionales dado que sus competencias se superponen en ocasiones.
- la medida en que los usuarios conocen sus derechos y la manera de hacerlos valer.
- la coordinación y cooperación entre los estados miembros y entre éstos y terceros países sobre el derecho nacional aplicable en cada caso.

A pesar que los esfuerzos por regular el envío de spam y que hacen mucho hincapié en la adopción de medidas complementarias a las existentes para reforzar el cumplimiento de la normativa y aumentar la cooperación a nivel nacional entre la administración pública y la industria, lo cierto es, que fijar una política de precios aplicada sobre la comunicación comercial y cuyo coste económico previamente estipulado recayese directamente en su emisor podría constituir una medida eficaz de persuasión para el envío de spam.

Conclusiones

Internet ha llegado a ser progresivamente un medio de comunicación mundial y actualmente presenta oportunidades sin precedentes para el desarrollo del comercio global y de una economía integrada a escala mundial.

Los avances experimentados en pocos años en el marco de la Sociedad de la Información dotan al ciudadano del mayor grado de desarrollo económico, social, cultural e individual conocido hasta el momento. Los beneficios de las TIC son cuantiosos y considerables tanto a nivel individual como organizativo.

Lamentablemente el desarrollo de las tecnologías de Internet ha supuesto un nuevo entorno para la delincuencia hasta el punto de provocar una evolución tecnológica a nivel de las estafas tradicionales. En este sentido las TIC han favorecido la comisión de delitos a gran escala, con mayor eficiencia y, por lo general, con mayor impunidad para el infractor dada la dificultad de perseguir este tipo de conductas ilícitas.

Individualmente todos debemos ser conscientes de la magnitud del problema y buscar niveles adecuados de formación, sensibilización e información y, con el compromiso adecuado y la ayuda de las empresas y los poderes públicos, adoptar medidas eficientes a fin de mantener actualizados los sistemas de información y denunciar los casos de infracción existentes para que puedan ser sancionados.

A pesar de las medidas de protección que se puedan establecer la mayor parte de los ataques a la seguridad de las redes no se pueden evitar sin la concienciación de los usuarios. La concienciación y la formación de los usuarios referida al uso y abuso de Internet deben ser prioritarias, deben ser planificadas y dirigidas a la sociedad en su conjunto.

Los legisladores han tratado buscar el equilibrio entre los deseos de los contrarios al spam que defienden el derecho fundamental a la privacidad y los partidarios del spam que defienden el derecho a la libertad de información por cualquier medio de difusión, el derecho a la libertad de empresa y a las necesidades económicas de un mercado que no renuncia a esta nueva modalidad publicitaria y que, de ser prohibida su práctica en unos países, podría colocar a sus empresas en inferioridad de condiciones competitivas respecto de otras empresas residentes en otros países que sí la autoriza.

Las comunicaciones comerciales electrónicas pueden ser un importante mecanismo a través del cual las empresas se anuncien y atraigan clientes en el entorno en línea.

El problema es que las comunicaciones comerciales no solicitadas por correo electrónico han alcanzado proporciones inquietantes llegando a constituir uno de los retos principales a los que se enfrenta Internet y la Sociedad de la Información.

Frente a este problema se reconoce el derecho a las protecciones de la vida privada, en particular, frente a ciertas técnicas de comunicación especialmente insistentes y agresivas: el spam.

Su recepción puede derivar en costes para los destinatarios tales como gastos de almacenamiento, tiempo invertido y ralentización del servicio de acceso a Internet.

Muchos remitentes de spam emplean procedimientos ilícitos durante la recolección de datos personales, sin el consentimiento de los titulares y sin informar del uso y tratamiento que tendrán los mismos. Además emplean el spam como medio de difusión de técnicas delictivas, si cabe, más preocupantes como el phishing.

Los datos personales de los de la Red poseen una notable trascendencia respecto de la actividad comercial. Particularmente la obtención y el tratamiento de la información que permite identificar o hacer identificable a un determinado sujeto en línea es la etapa previa y necesaria para poder difundir las comunicaciones comerciales. Implica no únicamente respetar los principios normativos que rigen la publicidad en línea sino además los vigentes en materia de protección de datos de carácter personal.

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 a ésta, de modo libre, inequívoco e informado su conformidad.

En el supuesto en que la finalidad que justifique el tratamiento de la información personal sea la difusión publicitaria, la LOPD prevé la utilización de los datos personales recabados con fines comerciales tanto de fuentes accesibles al público como resultado del consentimiento previo del titular, no siendo necesario la conformidad en aquellos casos en los que se hubiera mantenido una relación negocial, laboral o administrativa con la entidad que recaba la información.

Las comunicaciones comerciales se deben identificar como tales al igual que la persona física o jurídica en nombre de la cual se realiza el envío publicitario.

Mientras que algunos emisores de spam proporcionan a los destinatarios modos sencillos y gratuitos de rechazar envíos futuros de spam otros no proporcionan mecanismo alguno o se niegan a cumplir la normativa reguladora del spam ocultando la procedencia del mensaje o no identificando como publicidad el mensaje.

El envío de spam 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. Redes, cuyo medio Internet caracterizado por la ausencia de limitaciones temporales, la falta de delimitación territorial o la diversidad de materias afectadas, va a dificultar cualquier intento normativo.

Es por esto que la excesiva dispersión normativa (LOPD, Reglamento de desarrollo de la LOPD, LSSICE, LGT, Ley de Competencia Desleal, directivas, comunicaciones, entre otras,) constituye un entramado jurídico ciertamente complejo en relación a las comunicaciones comerciales.

La regla general es que las comunicaciones comerciales remitidas a través de las redes electrónicas se adecuen a las normas publicitarias vigentes y de aplicación en el estado desde el que se difunden, 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 no solicitada queda exceptuada al establecerse la posibilidad de que un estado miembro limite o impida dicha publicidad aún en el caso de que el envío sea lícito en el país de origen.

No obstante el problema sigue pendiente respecto del envío de publicidad no solicitada procedente de estados no miembros del EEE o la UE no obligados al cumplimiento de directivas comunitarias. La solución pasa por la autorregulación.

Por último, en España, el envío de publicidad comercial no solicitado se prohíbe en aquellos casos en los que de modo previo no se ha sido solicitado ni expresamente autorizado y no hubiese existido una relación contractual entre la entidad o el sujeto anunciante y el destinatario de la comunicación comercial.

Bibliografía

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS*. Guía para la lucha contra el spam*.
- APARICIO VAQUERO, Juan Carlos. Régimen jurídico de las comunicaciones comerciales realizadas a través del correo electrónico. En *La Ley: revista jurídica española de doctrina, jurisprudencia y bibliografía*, núm. 4, 2005, pp. 1476-1489.
- ASOCIACIÓN ESPAÑOLA DE COMERCIO ELECTRÓNICO, ASOCIACIÓN PARA LA AUTORREGULACIÓN DE LA COMUNICACIÓN COMERCIAL. *Código Ético de Comercio Electrónico y Publicidad Interactiva*, 2002.
- ASOCIACIÓN PARA LA INVESTIGACIÓN DE MEDIOS DE COMUNICACIÓN. *Navegantes en la Red: 11ª encuesta a usuarios de Internet*, 2009.
- FUNDACIÓN TELEFÓNICA. *La Sociedad de la Información en España 2009: 10 años de Sociedad de Información*, 2009.
- GÓMEZ-JUÁREZ SIDERA, Isidro. Consideraciones sobre el régimen jurídico del "spam" con ocasión del nuevo artículo 29.2 de la Ley de Competencia Desleal. En *Datospersonales.org: la revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 46, 2010.
- GONZÁLEZ DE LA GARZA, Luís María. *Sociedad de la información en Europa*. Madrid: Reus, 2008.
- GUILLÉN CATALÁN, Raquel. *Spam y comunicaciones comerciales no solicitadas*. Navarra: Aranzadi, 2005.
- INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. *Estudio sobre usuarios y entidades públicas y privadas afectadas por la práctica fraudulenta conocida como phishing*, 2007.

- PLAZA SOLER, Juan Carlos. La regulación de los correos electrónicos comerciales no solicitados en el derecho español, europeo y estadounidense. En *Revista del poder judicial*, núm. 68, 2002.
  - Los correos electrónicos comerciales no solicitados un año después de la LSSICE. En *Revista de la contratación electrónica*, núm. 45, 2004, pp. 3-37.
- RIVERO GONZÁLEZ, María Dolores. Régimen jurídico de la publicidad en Internet y las comunicaciones comerciales no solicitadas por correo electrónico. En *Revista de derecho mercantil*, núm. 250, 2003, págs. 1587-1614.
- ROMERO JAIME, Diego Jesús. Del charlatán al spam: publicidad molesta y libertad informática. Tutela judicial del consumidor y acciones de cesación. En *Boletín de información del Ministerio de Justicia*, núm. 2066, 2008, pp. 2537-2564.
- SÁNCHEZ DEL CASTILLO, Vilma. *La publicidad en Internet: régimen jurídico de las comunicaciones comerciales electrónicas*. Madrid: La Ley, 2007.
- SECRETARÍA DE ESTADO DE TELECOMUNICACIONES Y PARA LA SOCIEDAD DE LA INFORMACIÓN. *La sociedad en Red 2008: informe anual*, 2009.
- TAPIA GUTIÉRREZ, Paloma. Informe sobre las comunicaciones comerciales no solicitadas efectuadas por correo electrónico: estudio comparativo de la "Unsolicited Commercial Electronic Mail Act" norteamericana de 14 de febrero de 2001 y del anteproyecto español de Ley de Comercio Electrónico. En *Estudios sobre consumo*, núm. 57,2001, pp. 105-118.
- VÁZQUEZ RUANO, Trinidad. *La protección de los destinatarios de las comunicaciones comerciales electrónicas*. Madrid: Marcial Pons, 2008.

Leyes, directivas, comunicaciones, etc.

- Ley 34/1988, de 11 de noviembre de 1988, General de Publicidad.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos.
- Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Ley 29/2009, de 30 de diciembre, por la que se modifica el régimen legal de la competencia desleal y de la publicidad para la mejora de la protección de consumidores y usuarios.
- Directiva 84/450/CEE del Consejo, de 10 de septiembre de 1984, relativa a las aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de publicidad engañosa.
- 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 esos 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 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 el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

- 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 2002/58/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 2005/29/CE del Parlamento Europeo y del Consejo, de 11 de mayo de 2005, relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) nº 2006/2004 del Parlamento Europeo y del Consejo (Directiva sobre las prácticas comerciales desleales).
- Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE, adoptado el 27 de febrero de 2004.
- Dictamen 1/2009 sobre las propuestas que modifican la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

- 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. *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*, 2001.
- 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. *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. *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 entre las autoridades nacionales encargadas de la aplicación de la legislación en materia de protección de consumidores. (*Reglamento 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. *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 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 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 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, consultado el [2/08/2010]