COMISIÓN DE LAS COMUNIDADES EUROPEAS

Bruselas, 22.01.2004
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

ÍNDICE

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*

(Texto pertinente a efectos del EEE)

RESUMEN

Las comunicaciones comerciales no solicitadas por correo electrónico, también denominadas *spam*, han alcanzado proporciones inquietantes. Se considera que actualmente más del 50 % del tráfico de correo electrónico a nivel mundial está constituido por *spam*. Y aún más inquietante resulta el índice de crecimiento de este fenómeno, puesto que en 2001 la proporción de *spam* era de «solamente» el 7 %.

El *spam* constituye un problema desde muy diversos puntos de vista: intimidad, fraude a los consumidores, protección de los menores y de la dignidad humana, costes suplementarios para las empresas, pérdida de productividad. Más en general, el fenómeno socava la confianza de los consumidores, algo indispensable para el éxito del comercio electrónico, de los servicios en línea e, incluso, de la sociedad de la información.

La UE previó este riesgo, adoptando en julio de 2002 la Directiva 2002/58/CE sobre la intimidad y las comunicaciones electrónicas, que introdujo en el conjunto de la UE el principio del consentimiento previo («registro de inclusión») para el envío de correo electrónico con fines comerciales (incluidos mensajes SMS o MMS enviados a teléfonos móviles), así como garantías complementarias para los consumidores. El plazo para la aplicación de dicha Directiva concluyó el 31 de octubre de 2003. Se han abierto procedimientos de infracción contra varios Estados miembros que no han notificado a la Comisión sus medidas de transposición.

La aprobación de la legislación constituye un primer paso imprescindible, pero es sólo una parte de la solución. La presente Comunicación enumera una serie de acciones necesarias para completar la normativa de la UE y hacer realidad la «prohibición del *spam*».

No hay, desgraciadamente, un remedio milagroso contra el *spam*. Las acciones enumeradas en la presente Comunicación se centran, en particular, en el cumplimiento efectivo de la legislación por los Estados miembros y las autoridades públicas, en las soluciones técnicas y la autorregulación por parte de la industria y en la sensibilización de los consumidores. También se subraya la dimensión internacional, dado que una gran cantidad de *spam* procede del exterior de la Unión Europea.

Aunque estas acciones reflejan en términos generales el consenso que se alcanzó durante 2003, confirmado en un seminario público que tuvo lugar en octubre de dicho año, también será esencial alcanzar un consenso sobre su aplicación. Sólo podrá frenarse la proliferación del *spam* si todos los interesados, desde los Estados miembros y las autoridades públicas hasta los consumidores y los usuarios de Internet y las

comunicaciones electrónicas, pasando por las empresas, desempeñan el papel que les corresponde.

Algunas de las acciones mencionadas tienen un coste evidente, pero es el precio que debe pagarse si se quiere que el correo electrónico y los servicios electrónicos sigan constituyendo una herramienta de comunicación eficiente. La aplicación de las acciones enumeradas en la presente Comunicación contribuirá en buena medida a reducir el volumen de *spam*, en beneficio de la sociedad de la información, de nuestros ciudadanos y de nuestras economías.

Antecedentes y finalidad

Nadie duda de que el envío por correo electrónico de comunicaciones comerciales no solicitadas[1], también denominado *spam* o correo basura, constituye uno de los problemas más graves que conoce Internet actualmente. Es un fenómeno que ha alcanzado proporciones inquietantes y podría inducir a los usuarios actuales de mensajes electrónicos o SMS a dejar de utilizar el servicio de correo electrónico –que es una de las aplicaciones más populares de Internet– o los servicios móviles, o a utilizarlos de manera más restringida. Más en general, el *spam* exige una atención aún mayor si se tiene presente que, según lo previsto, Internet y otros medios de comunicaciones electrónicas (p. ej., el acceso de banda ancha, el acceso inalámbrico o las comunicaciones móviles) deben constituir un elemento esencial del crecimiento de la productividad en una economía moderna.

Aunque existe consenso sobre la necesidad de actuar antes de que la proliferación del *spam* contrarreste las ventajas que aportan a empresas y particulares el servicio de correo electrónico y los demás servicios electrónicos, no resulta fácil determinar cuál es la mejor forma de combatirlo. Y lo que es más importante, no existen remedios milagrosos. Sólo podrá frenarse eficazmente la proliferación del *spam* si todos los interesados, desde los Estados miembros y las autoridades competentes hasta los consumidores y los usuarios de Internet y las comunicaciones electrónicas, pasando por las empresas, desempeñan el papel que les corresponde.

La presente Comunicación enumera una serie de acciones que deberían realizarse en distintos frentes (jurídico, técnico y de sensibilización), basándose en la Directiva 2002/58/CE, que establece un régimen de consentimiento previo («lista de inclusión») que los Estados miembros debían aplicar para las comunicaciones comerciales a más tardar el 31 de octubre de 2003[2].

Esta serie de acciones se centra, en particular, en la aplicación efectiva de la Directiva por los Estados miembros y el cumplimiento de sus disposiciones, en las medidas técnicas, en la autorregulación del sector, en la sensibilización de los consumidores y en la cooperación internacional. La dimensión internacional resulta ciertamente crucial, dado que un volumen considerable de *spam* parece proceder del exterior de la Unión Europea, y en particular de Norteamérica[3].

---

1 La presente Comunicación no cubre las comunicaciones no solicitadas fuera de línea, como el correo (postal) no solicitado.

2 Véase en particular el artículo 13 de la Directiva 2002/58/CE sobre la intimidad y las comunicaciones electrónicas (véase la sección 2).

3 Por ejemplo, las iniciativas de «buzón de *spam*» organizadas en 2002 respectivamente por la «Commission Nationale Informatique et Libertés (CNIL)» en Francia y por la «Commission de la

Estas acciones reflejan en términos generales el consenso alcanzado durante el año 2003, según quedó confirmado en el seminario público organizado en octubre de 2003[4]. Un consenso en este ámbito es tanto más importante cuanto que corresponde esencialmente a las partes interesadas, con el apoyo de la Comisión en la medida de lo posible, aplicar las acciones enumeradas, en beneficio de la sociedad de la información, la industria y los usuarios.

Estructura del documento

El documento examina distintos aspectos del problema y propone medidas específicas para abordar cada uno de ellos. También se ponen de relieve las mejores prácticas cuando parece útil.

Las acciones propuestas se presentan según la siguiente estructura:

– **Acciones de aplicación y de cumplimiento**: van dirigidas principalmente a los Gobiernos y a las autoridades públicas, en ámbitos tales como recursos y sanciones, mecanismos de denuncia, denuncias transfronterizas, cooperación con terceros países y seguimiento (sección 3).

– **Acciones de autorregulación y acciones técnicas:** se refieren sobre todo a los agentes del mercado, en ámbitos tales como disposiciones contractuales, códigos de conducta, prácticas de comercialización aceptables, etiquetas, mecanismos alternativos de solución de litigios, soluciones técnicas como el filtrado y seguridad (sección 4).

– **Acciones de sensibilización**: engloban los mecanismos de prevención, educación de los consumidores y notificación que deben adoptar los Gobiernos y las autoridades públicas, los agentes del mercado, las asociaciones de consumidores y equivalentes (sección 5).

Todas estas acciones se resumen en un cuadro que figura al final de la presente Comunicación. Guardan relación entre sí de varias maneras, por lo que convendría en la medida de lo posible aplicarlas en paralelo y de manera integrada.

Antes de presentar estas acciones, en las secciones siguientes se analiza brevemente el fenómeno de *spam* como tal (sección 1) y se recuerdan las nuevas normas aplicables desde el 31 de octubre de 2003 (sección 2).

Protection de la Vie Privée (CPVP)» en Bélgica parecen confirmar que Estados Unidos y, en menor medida, Canadá, son la principal fuente de *spam*. Las conclusiones de la CPVP pueden consultarse en: http://www.privacy.fgov.be/publications/*spam*_4-7-03_fr.pdf; y el informe de la CNIL en: http://www.cnil.fr/thematic/docs/internet/boite_a_*spam*.pdf. Véase también: UNCTAD, Informe sobre el comercio electrónico y el desarrollo 2003, Nueva York y Ginebra, 2003, p. 27.

[4] Se distribuyó un documento de reflexión sobre las comunicaciones comerciales no solicitadas o *spam* antes del seminario. Este documento de reflexión estaba basado a su vez en debates previos en el marco del Comité de Comunicaciones (COCOM) y con el Grupo de trabajo sobre protección de datos del artículo 29. Los miembros del COCOM y del Grupo de trabajo ofrecieron sus opiniones a través de un cuestionario. También reaccionaron varias asociaciones sectoriales y empresas, desde proveedores de servicios de Internet y operadores de comunicaciones (móviles y fijas) a fabricantes de equipos y programas informáticos, pasando por empresas de venta directa y publicidad.

1. EL PROBLEMA DEL *SPAM*

¿Qué es el *spam*?

El término *spam* se utiliza más que se define. En pocas palabras, este término suele usarse para designar el envío, a menudo masivo, de mensajes electrónicos no solicitados. La nueva Directiva no define el término *spam* ni lo utiliza. Recurre a los conceptos de «comunicaciones no solicitadas» transmitidas por «correo electrónico» «con fines de venta directa» que, conjuntamente, cubren de hecho la mayoría de los tipos de *spam*. El concepto de *spam* se utiliza, pues, en la presente Comunicación como sinónimo de «correo electrónico comercial no solicitado».

Conviene observar que el concepto de «correo electrónico» cubre no sólo los mensajes electrónicos tradicionales que utilizan el protocolo SMTP, sino también los SMS, los MMS y cualquier forma de comunicación electrónica en la que no se requiera la participación simultánea del remitente y el destinatario (véase la sección 2).

1.1. Amplitud del problema

El *spam* ha alcanzado proporciones inquietantes. Aunque las estadísticas varían, se considera generalmente que más del 50 % del tráfico de correo electrónico a escala planetaria está constituido por *spam*.

El ritmo de crecimiento de este fenómeno es aún más preocupante. Se calcula que en 2001 el *spam* representaba sólo un 7 % del tráfico mundial de correo electrónico. La cifra pasó al 29 % en 2002, y las proyecciones para 2003 predicen un 51 %.

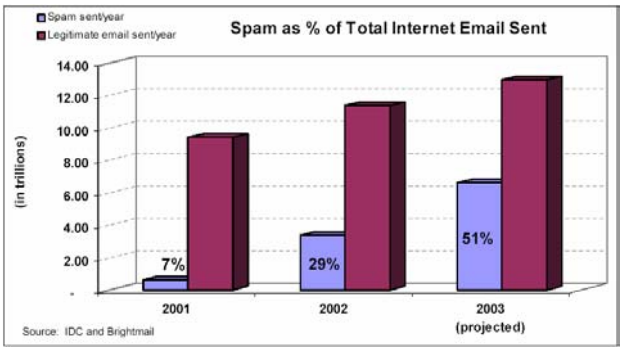

Figura 1: Proporción de *spam* en el total del correo electrónico enviado por Internet

Puede haber variaciones considerables entre las categorías de usuarios y entre las regiones del mundo (en la Comisión Europea, por ejemplo, se considera que un 30% de los mensajes electrónicos procedentes del exterior son *spam*). En general, no obstante, las cifras recientes relativas a la UE no son menos preocupantes que las cifras mundiales[5].

Aunque las comunicaciones no solicitadas o *spam* parecen plantear actualmente menos problemas en las redes móviles (por medio del servicio SMS, por ejemplo), tendencias tales como la transmisión por móvil de correo electrónico podrían incrementar el

volumen de *spam*. La experiencia de los países que conocen un intensa utilización del i-mode, como Japón, confirma esta amenaza.

---

[5] En septiembre de 2003, se estimó que la proporción de *spam* en la UE ascendía al 49 %, frente a un 54 % para el mundo en su totalidad (fuente: Brightmail, 2003).

1.2. ¿Por qué el *spam* constituye un problema?

Desde el punto de vista del individuo, el *spam* representa una intrusión en su intimidad. Esta consideración preside las nuevas normas sobre comunicaciones no solicitadas descritas en la sección siguiente. Además, el *spam* a menudo induce a error o a engaño. Una proporción considerable de *spam* parece responder a una voluntad de estafar a los consumidores mediante afirmaciones que inducen a error o a engaño[6], y lamentablemente demasiados consumidores responden a este tipo de *spam*[7]. Los mensajes de carácter pornográfico pueden resultar también perturbadores[8]. La limpieza de los buzones electrónicos lleva su tiempo y ocasiona gastos al usuario si se ve obligado a adquirir programas informáticos de filtrado u otros.

¿Le importa a la gente?

El número de denuncias sirve de indicador de las inquietudes de los usuarios. En 3 meses, el «buzón de *spam*» de Francia atrajo 325 000 mensajes. La experiencia similar de Bélgica obtuvo 50 000 denuncias en 2,5 meses[1]. El buzón de *spam* permanente de la FTC, denominado «base de datos UCE», recibía 130 000 mensajes diarios a principios de 2003[1].

Se ha llegado a un punto en que el *spam* genera también costes considerables para las empresas. En primer lugar, costes directos: el personal se ve obligado a limpiar las bandejas de entrada, lo que reduce su rendimiento y su productividad en el trabajo, los departamentos de informática dedican tiempo y dinero a intentar solucionar el problema, los proveedores de servicios de Internet (ISP) y de servicios de correo electrónico (ESP) deben adquirir más ancho de banda y más capacidad de almacenamiento para mensajes electrónicos no deseados. Se corre también el riesgo de que el *spam* ponga en juego la

---

6 Según un reciente informe de la FTC de Estados Unidos, un 22% del *spam* analizado contenía información falsa en el «asunto» del mensaje; el 42% contenía en dicho campo alegaciones engañosas que hacían pensar que el remitente tenía relaciones comerciales o personales con el destinatario; el 4 % del *spam* contenía información falsa en el «remitente» o el «asunto»; más de la mitad del *spam* vinculado a cuestiones económicas contenía información falsa en el «remitente» o el «asunto»; en un 40% de los casos, el cuerpo del mensaje contenía indicios de falsedad; el 90% de las ofertas relativas a inversiones u oportunidades comerciales contenían afirmaciones probablemente falsas; el 66 % del *spam* contenía información falsa en el «remitente», en el «asunto» o en el cuerpo del mensaje. (False Claims in Spam, A report by the FTC's Division of Marketing Practices, 30 de abril de 2003, disponible en: http://www.ftc.gov/reports/spam/030429spamreport.pdf).

7 Según Pew Internet, el 7% de los usuarios del correo electrónico declaran haber hecho un pedido tras recibir un mensaje electrónico no solicitado, y el 33% pulsó un enlace incluido en un mensaje electrónico no solicitado para obtener más información. Aunque el porcentaje de consumidores estafados sea relativamente bajo, el problema adquiere una nueva dimensión debido a las fenomenales economías de escala que pueden realizar operadores sin escrúpulos recurriendo a *spam* que induce a engaño o error. Véase: «Spam–How It Is Hurting Email and Degrading Life on the Internet, October 2003», informe de Deborah Fallows para el Pew Internet & American Life Project que se puede consultar en la dirección: http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf. Un remitente de correo electrónico masivo declaró recientemente, en el foro sobre *spam* organizado por la FTC en abril-mayo de 2003, que podía obtener beneficios aunque su porcentaje de respuestas fuera inferior al 0,0001%. (Observaciones de Timothy J. Muris, Chairman, Federal Trade Commission, Aspen Summit, Cyberspace and the American Dream, The Progress and Freedom Foundation, 19 de agosto de 2003 Aspen, Colorado).

8 A veces el *spam* contiene manifestaciones de violencia gratuita o incita al odio por razones vinculadas a la raza, el sexo, la religión o la nacionalidad.

responsabilidad de la entidad que lo recibe (p. ej., contenidos nocivos en el PC de un empleado), o que simplemente –de forma involuntaria– lo reenvíe (p. ej., inclusión errónea en una lista negra o perjuicio a su reputación). Existen también costes indirectos: algunos mensajes electrónicos legítimos de carácter comercial o profesional se dejan de recibir por obra de las técnicas de filtrado de *spam* actuales (los llamados «falsos positivos»), o simplemente no se leen a causa de su asociación con el *spam*. Además, el *spam* se utiliza cada vez más como vehículo de difusión de virus, que pueden resultar muy costosos para las empresas.

No es fácil calcular el coste del *spam*, especialmente para los particulares, entre otras cosas porque es difícil asignar un valor monetario a algunos de los perjuicios sufridos. No obstante, las estimaciones son inquietantes. Así por ejemplo, según Ferris Research en 2002 el *spam* costó a las empresas europeas 2 500 millones de euros solamente en pérdidas de productividad[9]. Y, como ya se ha indicado, el volumen de *spam* ha aumentado considerablemente con respecto a 2002. En junio de 2003, el proveedor de programas informáticos MessageLabs Ltd evaluó el coste del *spam* para las empresas británicas en aproximadamente 3 200 millones de libras[10]. El *spam* puede también tener consecuencias diferentes en distintos sectores. El sector jurídico, por ejemplo, puede verse especialmente afectado debido a la información confidencial y sensible que maneja.

Una de las consecuencias más inquietantes del *spam* es que socava la confianza de los usuarios, condición imprescindible para el éxito del comercio electrónico y de la sociedad de la información en su conjunto. Si cunde la idea de que un canal de venta está siendo utilizado por estafadores, las consecuencias para la reputación de los operadores legítimos del mismo sector pueden ser graves. Cifras recientes relativas a Estados Unidos, cuya experiencia en *spam* es más amplia que la de la UE, confirman que muchos usuarios pierden su confianza en el correo electrónico debido a las grandes cantidades de *spam* que reciben[11].

Más en general, se espera que Internet y otros medios de comunicaciones electrónicas –el acceso de banda ancha o el acceso inalámbrico– constituyan un elemento determinante del crecimiento de la productividad en las economías modernas. Ahora bien, en ausencia de medidas de seguridad adecuadas, algunas características interesantes de estos servicios –la conexión permanente, el acceso inalámbrico– pueden incrementar considerablemente el volumen de *spam* recibido o retransmitido. Así pues, el crecimiento de estos servicios podría implicar un aumento contraproducente del *spam* de no aplicarse rápidamente medidas eficaces.

---

9 Fuente: Ferris Research, 2003.

10 Esta cifra y otras estimaciones se mencionan en: «Spam; Report of an Inquiry by the All Party Internet Group», Londres, octubre de 2003, p. 8; este informe puede consultarse en la siguiente dirección: http://www.apig.org.uk .

11 Según la reciente investigación de Pew Internet antes citada, un 25 % de las personas interrogadas habían reducido su utilización del correo electrónico debido a la cantidad de *spam* que recibían.

2. RESUMEN DE LAS NORMAS RELATIVAS A LAS COMUNICACIONES COMERCIALES NO SOLICITADAS

2.1. El régimen del consentimiento previo (registro de inclusión)

La Directiva 2002/58/CE sobre la intimidad y las comunicaciones electrónicas (que debía transponerse a más tardar el 31 de octubre de 2003) exige que los Estados miembros prohíban el envío de mensajes comerciales no solicitados por correo electrónico u otro servicio de mensajería electrónica como el SMS o el MMS (*Multimedia Messaging Service*) salvo que se haya obtenido previamente el consentimiento del abonado a estos servicios de comunicaciones electrónicas (apartado 1 del artículo 13 de la Directiva)[12]. Se trata del sistema de consentimiento previo, que sólo era aplicable hasta ahora a los faxes y a los aparatos de llamada automática[13].

El nuevo régimen incluye tres normas fundamentales:

Norma n° 1: El envío de mensajes electrónicos con fines comerciales se supedita al consentimiento previo de los abonados. Se prevé una excepción limitada para los mensajes de correo electrónico (o SMS) enviados por una empresa a clientes existentes y referidos a servicios o productos similares. Este régimen se aplica a los abonados que son personas físicas, pero los Estados miembros pueden hacerlo extensivo a las personas jurídicas.

Norma n° 2: Es ilícito disimular u ocultar la identidad del remitente por cuenta de quien se efectúa la comunicación.

Norma n° 3: Todos los mensajes electrónicos deben mencionar una dirección de respuesta válida donde el abonado pueda pedir que no se le envíen más mensajes.

Sin embargo, no quedan prohibidos todos los mensajes electrónicos no solicitados. Está prevista una excepción a esta norma cuando los datos electrónicos para el envío de correo electrónico o SMS se hayan obtenido en el marco de una venta. Es lo que a veces se denomina "consentimiento previo suave". En el marco de la relación proveedor-cliente ya existente, la empresa que obtuvo los datos de un cliente puede utilizarlos con fines de comercialización de productos o servicios similares a los que ya le vendió. Esta excepción ha sido armonizada a escala comunitaria, y los Estados miembros no tienen más remedio que aplicarla. No obstante, debe formularse de manera estricta para no comprometer el funcionamiento del régimen de consentimiento previo. Sin embargo, incluso en este caso, la empresa debe indicar claramente, desde el momento en que obtiene los datos por vez primera, que éstos pueden ser utilizados con fines de venta directa (y, si procede, que pueden transmitirse a terceros a tal efecto) y ofrecer al consumidor la posibilidad de oponerse «sin gastos y de manera simple». Además, cada mensaje comercial posterior debe ofrecer al consumidor un medio simple y gratuito de detener el envío de nuevos mensajes (régimen de exclusión).

---

12 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 intimidad y las comunicaciones electrónicas) DO L 201 de 31.7.2002.

13 Para las llamadas de comercialización por telefonía vocal (excepto las de aparatos automáticos de llamada), los Estados miembros pueden elegir entre un enfoque de registro de inclusión o de registro de exclusión.

El régimen de consentimiento previo es obligatorio para todo envío de correo electrónico o SMS a una persona física con fines de venta directa. Los Estados miembros pueden extender el régimen de consentimiento previo a las comunicaciones destinadas a las empresas (personas jurídicas). Los Estados miembros que hubieran adoptado un régimen de exclusión para la comercialización entre empresas, incluido un sistema de registro de exclusión, pueden conservarlo. La aplicación de un régimen diferenciado en función de la naturaleza del abonado a un servicio de correo electrónico puede crear al remitente de mensajes dificultades para distinguir a las personas jurídicas de las físicas.

Para todas las categorías de destinatarios (personas físicas y jurídicas), la Directiva prohíbe el envío de mensajes de venta directa que oculten o disimulen la identidad del remitente. Los mensajes deben, además, mencionar una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones[14].

El «Grupo de trabajo sobre protección de datos del artículo 29», creado para asesorar a la Comisión y que reúne a las autoridades responsables de la protección de datos en la UE, está examinando con más detenimiento algunos de estos conceptos con el fin de contribuir a una aplicación uniforme de las medidas nacionales adoptadas en virtud de la Directiva 2002/58/CE[15]. Un consenso sobre estas cuestiones evitará diferencias de interpretación que perjudicarían al funcionamiento del mercado interior. En documentos previos del Grupo de trabajo se han abordado otros aspectos de las comunicaciones no solicitadas[16].

2.2. Cumplimiento de las disposiciones

Las disposiciones de la Directiva «general» sobre protección de datos relativas a recursos judiciales, responsabilidad y sanciones son aplicables a las disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas, incluidas las relativas a comunicaciones no solicitadas[17].

---

14 Apartado 4 del Artículo 13, de la Directiva 2002/58/CE.

15 De conformidad con lo dispuesto en el apartado 3 del artículo 15 de la Directiva 2002/58/CE, en conjunción con el artículo 30 de la Directiva 95/46/CE.

16 Véanse por ejemplo el dictamen 7/2000 sobre la propuesta de Directiva del Parlamento Europeo y el Consejo relativo al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, de 12 de julio de 2000 y la recomendación 2/2001 sobre algunos requisitos mínimos relativos a la recogida en línea de datos personales en la Unión Europea. La recolección de datos se examinó también en el documento de trabajo de 21 de noviembre de 2000 titulado «El respeto de la intimidad en Internet – Un enfoque europeo integrado sobre la protección de los datos en línea". Estos documentos pueden consultarse en la dirección: http://europa.eu.int/comm/internal_market/privacy/workingroup_en.htm.

17 El artículo 15 de la Directiva 2002/58/CE se remite al capítulo III de la Directiva 95/46/CE en materia de recursos judiciales, responsabilidad y sanciones:
Artículo 22 – Recursos
Sin perjuicio del recurso administrativo que pueda interponerse, en particular ante la autoridad de control mencionada en el artículo 28, y antes de acudir a la autoridad judicial, los Estados miembros establecerán que toda persona disponga de un recurso judicial en caso de violación de los derechos que le garanticen las disposiciones de Derecho nacional aplicables al tratamiento de que se trate.
Artículo 23 – Responsabilidad
1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.
2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad

En pocas palabras, los Estados miembros deben velar por que, en caso de infracción, existan vías de recurso y sanciones. Toda violación de los derechos garantizados por la legislación nacional debe ir acompañada del derecho individual a un recurso judicial. Aunque este recurso judicial debe entenderse sin perjuicio de posibles procedimientos administrativos (que pueden ser previos), no existe ninguna exigencia armonizada con respecto a éstos. Cualquier perjuicio sufrido a causa de un tratamiento o de un acto ilícitos debe ir acompañado de un derecho individual a una indemnización. Deben estar previstas sanciones en caso de infracción, con el fin de garantizar la plena aplicación de la Directiva.

Así pues, mientras una Directiva, por su propia naturaleza, concede a los Estados miembros cierto margen de maniobra en la elección de las medidas que adoptan para su aplicación –incluidos los recursos y las sanciones–, las medidas en sí son indispensables para garantizar la «plena aplicación» de las disposiciones relativas a las comunicaciones comerciales no solicitadas.

Como para cualquier Directiva, corresponde en primer lugar a los Estados miembros, y no a la Comisión, conseguir que se cumplan las disposiciones. Por ejemplo, no incumbe a la Comisión perseguir o imponer multas a los que violan los derechos y obligaciones previstos en la Directiva[18].

2.3. Otras disposiciones aplicables al *spam*

Una práctica a menudo vinculada al *spam* es la «recolección» de direcciones de correo electrónico, es decir, la recogida automática de datos personales en lugares públicos de Internet, p. ej. la web, las salas de charla, etc. Esta práctica es ilícita en virtud de la Directiva «general» sobre protección de datos 95/46/CE, esté o no efectuada de manera automática con ayuda de un programa informático[19].

El *spam* fraudulento y engañoso puede resultar especialmente desagradable. Estas prácticas son ya ilícitas en virtud de las normas existentes en la UE sobre publicidad engañosa y prácticas comerciales desleales (p. ej., la Directiva 84/450/CEE sobre publicidad engañosa)[20]. Generalmente, las leyes nacionales prevén también sanciones más severas en los casos más graves, incluidas sanciones penales.

---

si demuestra que no se le puede imputar el hecho que ha provocado el daño.
Artículo 24 – Sanciones
Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva.

18 Esta situación difiere de la de agencias como la Comisión Federal de Comercio de Estados Unidos.

19 Véase también el documento de trabajo del Grupo de trabajo sobre protección de datos del artículo 29 titulado «Privacy on the Internet» - An integrated EU Approach to On-line Data Protection" (Documento nº WP 37, adoptado el 21 de noviembre de 2000).

20 Directiva 84/450/CEE del Consejo, de 10 de septiembre de 1984, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de publicidad engañosa. DO L 250 de 19.9.1984, p. 17-20. La Comisión ha presentado recientemente una propuesta destinada a sustituir y actualizar esta Directiva (COM(2003) 356 final).

Determinados tipos de *spam* pueden resultar aún más perturbadores, sobre todo el pornográfico o con violencia gratuita, en particular cuando puede llegar a los niños[21]. Aunque el contenido de algunos de estos mensajes pueda ser nocivo, pero no ilícito, su distribución indiscriminada a niños y adultos suele ser ilícita en virtud del Derecho interno, previéndose a veces sanciones muy severas. Puede suceder que mensajes de *spam* lleven además un contenido ilícito, por ejemplo incitación al odio por motivos vinculados a la raza, el sexo, la religión o la nacionalidad. En cualquier caso, en cuanto estos mensajes persigan un objetivo de venta directa –como ocurre a menudo– quedan afectados por la prohibición del *spam*, al igual que otras categorías de correo electrónico no solicitado.

Es necesario también hacer referencia a la exigencia, prevista en 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 (Directiva sobre comercio electrónico), de que las «comunicaciones comerciales» deben ser claramente identificables como tales (letra a) del artículo 6 de la Directiva sobre comercio electrónico)[22].

Además, a menudo se perpetran actividades como la piratería o la suplantación de la identidad para facilitar el *spam*, con el fin de enviarlo o de acceder a bases de datos de direcciones o a ordenadores. Una gran parte de estas actividades estarán cubiertas por la Decisión marco relativa a los ataques contra los sistemas de información, que prevé sanciones penales. Esta Decisión marco, basada en una propuesta de la Comisión, fue objeto de un acuerdo político en febrero de 2003 y debería ser adoptada oficialmente en breve plazo[23]. En numerosos Estados miembros constituye ya delito penal el acceso ilícito a un servidor o un ordenador personal o su uso indebido.

---

21 El 24 de septiembre de 1998, el Consejo adoptó la Recomendación del Consejo de 24 de septiembre de 1998 relativa al desarrollo de la competitividad de la industria europea de servicios audiovisuales y de información mediante la promoción de marcos nacionales destinados a lograr un nivel de protección comparable y efectivo de los menores y de la dignidad humana (98/560/EC). Esta recomendación fue el primer instrumento jurídico adoptado en la UE sobre contenidos de los servicios audiovisuales y de información referido a todos los sistemas de entrega, de la radiodifusión a Internet.

22 Directiva del Parlamento Europeo y del Consejo de 8 de junio de 2000, DO L 178 de 17.7.2000. Por regla general, las «comunicaciones comerciales» deben respetar las disposiciones nacionales aplicables en el Estado miembro en que esté establecido el prestador de servicios. Esta norma no se aplica, sin embargo, a la licitud de las comunicaciones no solicitadas por correo electrónico (véase el artículo 3 de la Directiva sobre comercio electrónico y su anexo). En los casos (limitados) en que la Directiva 2002/58/CE no proteja a las personas físicas contra las comunicaciones comerciales no solicitadas (p. ej. personas físicas que no sean abonados), los Estados miembros deberán garantizar, con arreglo a la Directiva sobre comercio electrónico, que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente los registros de exclusión en los que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y los respeten (véase el artículo 7 de la Directiva sobre comercio electrónico).

23 Propuesta de Decisión marco del Consejo relativa a los ataques de los que son objeto los sistemas de información, COM(2002) 173 final, de 19.4.2002.

3. APLICACIÓN Y CUMPLIMIENTO EFECTIVOS A CARGO DE LOS ESTADOS MIEMBROS Y LAS AUTORIDADES PÚBLICAS

Esta sección se refiere a las acciones que se propone apliquen principalmente las administraciones y las autoridades públicas en ámbitos como recursos y sanciones, mecanismos de denuncia, denuncias transfronterizas, cooperación con terceros países y seguimiento.

No obstante, antes de entrar en la cuestión del cumplimiento, la Comisión observa que una serie de Estados miembros aún no han transpuesto la Directiva sobre la intimidad y las comunicaciones electrónicas, y en particular las disposiciones sobre correo electrónico comercial no solicitado que forman parte del nuevo marco regulador general de las comunicaciones electrónicas[24]. El Parlamento Europeo ha expresado recientemente su inquietud con respecto a este retraso[25]. Tras expirar el plazo de transposición de esta Directiva (31 de octubre de 2003), la Comisión incoó, en noviembre de 2003, procedimientos de infracción contra varios Estados miembros por ausencia de notificación de las medidas de transposición[26].

3.1. Introducción

La legislación impedirá que se envíe determinada cantidad de *spam*, pero no será suficiente por sí sola. La aplicación real del régimen de consentimiento previo debe ser prioritaria en todos los Estados miembros. Además de personal y recursos suficientes, resultarán necesarios unos mecanismos que aseguren el cumplimiento de la normativa, incluidos los de tipo transfronterizo. También resultará esencial la cooperación con los países no miembros de la UE. El seguimiento será igualmente importante, aunque solo sea para determinar las prioridades en materia de imposición.

Son varios los factores que parecen influir sobre la eficacia de los mecanismos de aplicación:

– la posibilidad de hacer cumplir la legislación por medio de multas u otras sanciones; algunas autoridades reguladoras carecen al parecer todavía de poderes coercitivos (reales);

– la naturaleza de 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 en este ámbito se superponen a veces;

– la medida en que los usuarios conocen sus derechos y la manera de hacerlos valer; es necesario indicar a los usuarios dónde presentar sus denuncias, los hechos que serán

---

24 Véase también del Noveno informe sobre la aplicación del conjunto de medidas reguladoras de las telecomunicaciones, disponible en la dirección: http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/9threport/index_en.htm.

25 La Comisión ha subrayado la importancia de aplicar plena, eficaz y puntualmente el nuevo marco regulador de las comunicaciones electrónicas, incluida la Directiva sobre la intimidad y las comunicaciones electrónicas, en su Comunicación «Comunicaciones electrónicas: el camino hacia la economía del conocimiento» (COM (2003) 65 de 11 de febrero de 2003).

26 Los escritos de requerimiento se enviaron el 25 de noviembre de 2003 (véase IP/03/1663).

objeto o no de investigación, los tipos de acciones que pueden emprenderse y la información que deben facilitar a las autoridades para poner en marcha una investigación;

– la coordinación y la cooperación entre los Estados miembros y entre éstos y terceros países sobre el Derecho nacional aplicable en casos concretos;

– los recursos disponibles para detectar a los remitentes de *spam* activos en la UE o fuera de ella y que ocultan su identidad, en particular sirviéndose de la identidad, las direcciones o los servidores de otros usuarios.

Las medidas aplicables para hacer cumplir las disposiciones relativas a las comunicaciones no solicitadas se han mencionado en la sección 2.2. Hasta el momento, los procedimientos relativos al correo electrónico comercial no solicitado se han administrado y organizado de manera muy dispar[27]. Aunque el hecho de utilizar como instrumento una Directiva deja a los Estados miembros cierto margen de maniobra en la aplicación de sus disposiciones, es necesaria una aplicación efectiva, cualquiera que sea el método utilizado.

Diversidad en los Estados miembros

La autoridad encargada de hacer cumplir las disposiciones relativas a las comunicaciones comerciales no solicitadas no es la misma en todos los Estados miembros. En la mayoría de los casos, es la autoridad competente en materia de protección de datos (APD) la que asume la responsabilidad principal. En algunos países, no obstante, esta misión la cumple la autoridad nacional de reglamentación de las comunicaciones electrónicas (ANR). Y en otros, incumbe principalmente a las autoridades responsables de la protección de los consumidores (incluido el defensor del pueblo). A menudo habrá que contar con más de una autoridad en la ejecución de las disposiciones relativas a las comunicaciones no solicitadas. Además, el *spam* implica en muchos casos prácticas engañosas o fraudulentas. (Una minoría de Estados miembros no tienen autoridad de protección de los consumidores y la imposición de las normas corre a cargo de las asociaciones de consumidores o de los propios consumidores). El envío de *spam* está a menudo vinculado a infracciones de las normas sobre protección de datos, tales como la recolección de direcciones electrónicas, cuando no a actividades de ciberdelincuencia como la intrusión ilícita en PC o servidores. Las autoridades encargadas de hacer cumplir las disposiciones sobre este tema no son necesariamente las mismas, y aún menos a escala transfronteriza.

Excepto en un reducido número de Estados miembros, una denuncia no desemboca necesariamente en una investigación. Se recurre a veces a contactos previos, incluyendo consignas y orientaciones a las empresas, con cierto éxito. A veces esta fase previa a la denuncia corre a cargo del consumidor, que debe ponerse en contacto con la empresa en cuestión antes de presentar una denuncia. Algunos países, como el Reino Unido, recurren a la autorregulación para organizar esta primera fase de actuación. En algunos Estados miembros existen ya mecanismos de denuncia en el marco de una autorregulación. Es frecuente también que las autoridades actúen por propia iniciativa. El hecho de que una autoridad administrativa esté encargada especialmente de estas cuestiones no excluye normalmente el acceso directo al sistema judicial.

No todas las APD pueden actuar contra personas jurídicas, ni tampoco (hasta ahora) tienen la posibilidad de imponer sanciones. Para ello, deben iniciar un procedimiento ante las autoridades judiciales.

En Francia, la experiencia del «buzón de *spam*» condujo a la APD a seleccionar algunos asuntos y someterlos a las autoridades judiciales, sin mucho éxito. En Bélgica, una experiencia similar condujo a un

[27] Hay que señalar que las denuncias se refieren a menudo también a aspectos conexos, como el derecho de acceso a los datos personales y el derecho a oponerse al tratamiento de dichos datos.

intercambio de opiniones con los remitentes sospechosos y, en casos transfronterizos, a poner los hechos en conocimiento de las autoridades correspondientes de otros Estados de la UE o de la FTC en Estados Unidos.

Es frecuente considerar que el medio más eficaz para hacer aplicar el régimen de consentimiento previo lo constituye un enfoque equilibrado que incluya la legislación, la imposición de las normas y la autorregulación. Se invita a los Estados miembros a evaluar la eficacia de su mecanismo de cumplimiento, en particular sobre la base de las distintas acciones que se proponen a continuación (véanse las secciones 3.2 a 3.6).

Se invita asimismo a los Estados miembros a elaborar estrategias nacionales para garantizar la cooperación entre las autoridades responsables de la protección de datos (APD), las autoridades encargadas de la protección de los consumidores (APC) y las autoridades nacionales de reglamentación de las comunicaciones electrónicas (ANR), y a evitar el solapamiento de competencias y la duplicación de funciones entre las distintas autoridades.

Para facilitar y coordinar los intercambios de información y de mejores prácticas en materia de aplicación eficaz (p. ej., por lo que se refiere a denuncias, recursos, sanciones y cooperación internacional), los servicios de la Comisión han creado **un Grupo informal en línea sobre las comunicaciones comerciales no solicitadas**, con el apoyo de los Estados miembros y las autoridades responsables de la protección de datos. Este Grupo facilitará y coordinará también los trabajos sobre las demás acciones enumeradas en la presente Comunicación, como la sensibilización y las soluciones técnicas.

Los documentos redactados con motivo de los debates del Grupo serán, por regla general, sometidos al Comité de comunicaciones (COCOM) creado en virtud del marco regulador de las redes y los servicios de comunicaciones electrónicas y/o al Grupo de trabajo sobre protección de datos del artículo 29 para que adopten las medidas oportunas. El Grupo puede, en particular, elaborar criterios de evaluación comparativa de las distintas medidas que se propongan.

Este Grupo en línea incluye representantes de las administraciones nacionales competentes y de las autoridades encargadas de la protección de datos, así como de los servicios de la Comisión. El propio Grupo determinará cómo garantizar la participación de otras partes interesadas.

3.2. Recursos y sanciones eficaces

3.2.1. Análisis

Actualmente, las soluciones incluyen generalmente multas o un requerimiento de que se ponga fin al tratamiento ilícito de los datos, acompañado ocasionalmente del «bloqueo» de los sitios web implicados. En algunos Estados miembros, el requerimiento de poner fin al tratamiento precede o acompaña a la imposición de multas en caso de incumplimiento. Sin embargo, no todas las autoridades son competentes en relación con la totalidad de las infracciones relacionadas con el *spam*, ni tienen a su disposición las mismas herramientas. También es frecuente que los asuntos sean sometidos a las autoridades judiciales. Ahora bien, no todos los Estados miembros tienen previstas sanciones judiciales para este tipo de infracciones.

No todos los Estados miembros prevén vías de recurso y multas/sanciones en su Derecho administrativo o penal. Las sanciones penales varían de un Estado miembro a otro, incluyendo a veces penas de reclusión. Además, suele ser posible reclamar daños y perjuicios en procedimiento civil.

Aunque suele efectuarse una distinción entre infracciones leves y graves (p. ej., distribución masiva de mensajes, publicidad y prácticas comerciales engañosas o fraudulentas), las correspondientes sanciones varían mucho de un Estado miembro a otro.

En numerosos casos, las actividades de *spam* pueden también abordarse con las soluciones previstas por la legislación general sobre protección de datos (p. ej., violación de la obligación de notificar, del derecho de acceso, de la obligación de nombrar un representante en un Estado miembro de la UE, etc.) o por otra legislación específica (sobre publicidad engañosa, prácticas comerciales fraudulentas, etc.). Antes de la introducción del régimen de consentimiento previo, se utilizaron distintos argumentos jurídicos para combatir ciertas formas de *spam* (p. ej., las campañas de envío masivo de correo, el uso ilícito de datos personales, la perturbación de una red, el uso indebido de las cuentas de correo electrónico, el fraude o la interpretación errónea de un contrato).

Por regla general, la solución judicial no se considera un mecanismo de cumplimiento suficiente. Habitualmente la APD, la APC y/o la ANR pueden imponer multas administrativas, pero sus importes varían. Muchos Estados miembros en los que no existe actualmente esta posibilidad están estudiando su introducción. Por el contrario, las sanciones administrativas parecen adaptarse especialmente a este sector dinámico. Las propias APD, APC y ANR se sirven a menudo de instrumentos complementarios para hacer cumplir la normativa. Los procedimientos administrativos pueden resultar a la vez asequibles y rápidos (no más de 50 días, por ejemplo, según la APD italiana).

3.2.2. Acciones propuestas

Como condición previa, la Comisión invita a los Estados miembros que aún no han transpuesto la Directiva, y en particular sus disposiciones relativas a las comunicaciones no solicitadas, a hacerlo sin más demora. Los servicios de la Comisión están dispuestos a ayudar a los Estados miembros en caso de necesidad.

Se invita a los Estados miembros a evaluar la eficacia de su sistema de recursos y sanciones en caso de infracción, y a establecer posibilidades adecuadas de que las víctimas reclamen daños y perjuicios.

Los Estados miembros y las autoridades competentes que no tienen previstas soluciones administrativas deberían estudiar la implantación de este tipo de recurso contra el *spam*, que constituye un procedimiento rápido, asequible y eficaz para hacer aplicar el régimen de consentimiento previo.

La Comisión comprobará que las medidas de transposición nacionales prevean sanciones reales en caso de incumplimiento de la normativa por los agentes del mercado, incluyendo cuando proceda sanciones económicas y penales.

En este contexto, la Comisión examinará también en qué medida disponen las autoridades competentes de las facultades de investigación y ejecución necesarias.

3.3. Mecanismos de denuncia

3.3.1. Análisis

Una aplicación eficaz de las normas implica contar con unos mecanismos de denuncia adecuados. Algunas APD han establecido buzones electrónicos a los cuales pueden reenviar los usuarios los mensajes comerciales no solicitados, comprometiéndose a intervenir en casos determinados.

Algunos Estados miembros parecen preferir procedimientos administrativos normales y/o los contacto con los ISP o con los equipos nacionales de respuesta a emergencias informáticas (CERT) si hay perturbación de la red. Otros favorecen procedimientos más tradicionales (acción civil por daños y perjuicios/procedimientos administrativos). A veces se consideran preferibles la corregulación o la autorregulación a las medidas coercitivas.

Mejores prácticas

A finales de 2002, Francia y Bélgica establecieron buzones electrónicos para recibir denuncias precisas relativas al *spam*, con resultados muy interesantes. Existen informes sobre estas iniciativas a disposición del público[28]. Se espera que Francia adopte este sistema con carácter permanente en el marco de las nuevas normas que transponen la Directiva sobre la intimidad y las comunicaciones electrónicas. La Comisión Federal del Comercio (FTC) estadounidense explota un buzón electrónico de este tipo y utiliza sus resultados en sus acciones basadas en la legislación sobre prácticas comerciales desleales y engañosas[29].

Una de las ventajas de los buzones electrónicos es que parecen animar a los consumidores a denunciar las infracciones y contribuyen así a que la legislación adoptada se aplique más eficazmente. Por otro lado, pueden proporcionar estadísticas esenciales sobre la amplitud y la naturaleza de los problemas encontrados en un país o una región, construyendo así una panorámica que representa para las autoridades una herramienta preciosa para fijar o adaptar las prioridades al respecto. Además, pueden elaborarse acciones preventivas sobre la base de los conocimientos adquiridos. Así por ejemplo, el CNIL ha utilizado la información recogida durante su operación «buzón de *spam*» para elaborar expedientes informativos destinados a los usuarios y a los vendedores.

Naturalmente, la utilidad de un buzón electrónico en el seguimiento y la medición de la amplitud y el alcance del *spam* depende de la capacidad de investigar provechosa y rápidamente las denuncias presentadas.

Solo algunos Estados miembros parecen prever la posibilidad de utilizar este tipo de buzón electrónico, pese al interés que existe por aprender de la experiencia adquirida por otros Estados miembros con este método. Entre las razones que se aducen para ello figuran: la existencia de la posibilidad de presentar una denuncia por correo electrónico, en general a través del sitio web de la autoridad, la necesidad de disponer de personal

---

28 El informe de 24 de octubre de 2002 adoptado por la Commission National Informatique et Libertés (CNIL), APD francesa, está disponible en la dirección: http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/*spam*/*spam*_sommaire.htm
El informe adoptado en julio de 2003 por la Commission de Protection de la Vie Privée, APD belga, puede consultarse en: http://www.privacy.fgov.be/publications/*spam*_4-7-03_fr.pdf.

29 Véase por ejemplo http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf. Los mensajes no solicitados o engañosos pueden enviarse a la dirección: uce@ftc.gov.

especializado y equipos suplementarios y la necesidad de modificar los procedimientos jurídicos existentes.

3.3.2. Acciones propuestas

Los Estados miembros y las autoridades competentes deberían evaluar la eficacia de su ordenamiento jurídico para tratar las denuncias de los usuarios y adaptarlo si procede.

Se invita a los Estados miembros y las autoridades competentes a establecer buzones electrónicos especiales, acompañándolos de campañas informativas.

Estos buzones especiales deberían permitir la realización de investigaciones y análisis sencillos destinados a comprender mejor el problema y fijar prioridades en materia de cumplimiento de la normativa.

Los servicios de la Comisión facilitarán la difusión de la información sobre las experiencias con los buzones electrónicos.

3.4. Denuncias transfronterizas y cooperación en materia de cumplimiento dentro de la UE

3.4.1. Análisis

El tratamiento eficaz de las denuncias transfronterizas es uno de los elementos que harán posible la protección de los consumidores en este ámbito. Será esencial garantizar que puedan conectarse los mecanismos de denuncia nacionales, cualesquiera que sean sus modalidades, de modo que las denuncias formuladas por los usuarios de un Estado miembro referidas a mensajes procedentes de otro Estado miembro sean también atendidas con eficacia (véase el punto 3.5 sobre cooperación con los terceros países).

Hoy en día, no todos los Estados miembros disponen de un procedimiento oficial para tratar las denuncias transfronterizas. Entre las soluciones actualmente utilizadas cabe citar los contactos con la autoridad competente de otro Estado miembro y la posibilidad de transferir la denuncia a la autoridad competente del Estado en el que se originó el mensaje.

A nivel europeo, las APD (incluidas las del EEE y los países candidatos) procuran intercambiar información sobre las denuncias transfronterizas por medio del «seminario de tratamiento de denuncias», grupo creado en el marco de la Conferencia Europea de Comisarios sobre Protección de Datos. Es posible recurrir a él en caso de denuncias transfronterizas relativas a *spam*, y en particular para determinar la legislación aplicable en casos concretos. No obstante, hay que decir que no todas las APD aplican las disposiciones sobre comunicaciones no solicitadas.

En el ámbito de la protección de los consumidores, la Comisión ha propuesto recientemente un Reglamento relativo a la cooperación entre las autoridades nacionales encargadas de la aplicación de la legislación en materia de protección de los consumidores para abordar los problemas transfronterizos[30].

[30] COM (2003) 443 final.

El Reglamento establece procedimientos de asistencia mutua y prevé una cooperación operativa más intensa entre las autoridades nacionales. Quedaría cubierto por el régimen propuesto el *spam* que induzca a error o engaño o que infrinja otras normas en el ámbito de la protección de los consumidores, aunque no todo el *spam* prohibido por la Directiva sobre la intimidad y las comunicaciones electrónicas. El Consejo y el Parlamento examinan actualmente este Reglamento.

3.4.2. Acciones propuestas

Se invita a los Estados miembros y las autoridades competentes a evaluar la eficacia de sus actuales procedimientos de tratamiento de las denuncias transfronterizas (acuerdos de asistencia mutua, por ejemplo).

Se insta a las administraciones nacionales competentes a intensificar la coordinación. Se incluye la coordinación y el intercambio de información entre las autoridades encargadas de hacer cumplir las nuevas disposiciones, y entre éstas y las responsables de formas particulares de *spam* (p. ej., el *spam* fraudulento o «scam», el *spam* pornográfico, los mensajes sobre productos relacionados con la salud ilícitamente distribuidos).

Por lo que se refiere al *spam* fraudulento y engañoso, se urge al Consejo y al Parlamento a aprobar el Reglamento propuesto sobre cooperación en materia de protección de los consumidores lo más rápidamente posible para que las autoridades de la UE encargadas de la protección de los consumidores dispongan de todas las herramientas necesarias para hacer frente al *spam* que induce a error o engaño. Se les invita también a examinar la posibilidad de extender el ámbito de aplicación de dicho Reglamento a la Directiva sobre la intimidad y las comunicaciones electrónicas.

Se invita a los Estados miembros a estudiar los medios de suprimir los obstáculos existentes al intercambio de información y a la cooperación, así como la posibilidad de pedir que adopten medidas a sus homólogos de otros Estados miembros. En la práctica, podría ser útil disponer de un mecanismo de enlace (véase la iniciativa antes citada de las APD) en cuyo marco pudieran cooperar los reguladores nacionales para garantizar la aplicación transfronteriza. El establecimiento de una red de apoyo a la cooperación podría basarse en programas de la Comisión ya existentes, como IDA[31].

La Comisión se propone facilitar y promover estos esfuerzos de coordinación entre las autoridades nacionales competentes, en particular a través del Grupo informal en línea sobre comunicaciones comerciales no solicitadas que acaba de crearse. Los servicios de la Comisión han comenzado a examinar, con ayuda de los Estados miembros y las autoridades nacionales afectadas, qué acciones concretas serían necesarias para mejorar el tratamiento de las denuncias transfronterizas. Las conversaciones con las autoridades nacionales proseguirán a lo largo del año 2004.

3.5. Cooperación con los terceros países

3.5.1. Análisis

Las nuevas normas son de aplicación al tratamiento de los datos personales en el marco de la prestación de servicios de comunicaciones electrónicas accesibles al público en las

[31] Se encontrará información sobre el programa IDA en la dirección: http://europa.eu.int/comm/enterprise/ida/index.htm.

redes públicas de comunicaciones en la Unión Europea (y en el EEE). Por lo tanto, el artículo 13 de la Directiva 2002/58/CE, que establece la norma del consentimiento previo, se aplica a todas las comunicaciones comerciales no solicitadas con destino u origen en redes que se encuentran en la Unión Europea (y en el EEE). Así pues, los mensajes procedente de terceros países deben ajustarse también a las normas de la UE, al igual que los mensajes procedentes de la UE y enviados a destinatarios en terceros países.

La aplicación efectiva de la norma a los mensajes procedentes de terceros países será, sin duda, más complicada que en el caso de los mensajes originados en la UE. Sin embargo, reviste una importancia capital, ya que gran parte del *spam* procede del exterior de la UE.

Aunque para ello será necesario disponer de una panoplia de instrumentos tales como medidas de prevención, técnicas de filtrado, medidas de autorregulación, disposiciones contractuales y medidas de cooperación internacional, la presente sección se centra en esta última. El primer objetivo de la cooperación internacional es promover la aprobación de una legislación eficaz en los terceros países. El segundo, cooperar con estos países para garantizar que las normas aprobadas se apliquen realmente.

No se cuenta con mucha experiencia sobre la imposición de las normas de registro de inclusión o de exclusión a las comunicaciones procedentes del exterior de la UE. Entre los obstáculos existentes suele citarse, además del hecho de que el *spam* sea un fenómeno relativamente nuevo, la dificultad para identificar a los remitentes del *spam* o los esfuerzos necesarios para conseguirlo, la falta de mecanismos internacionales de cooperación (apropiados) y la ausencia de competencias en asuntos internacionales de algunas autoridades.

Por lo que se refiere al *spam* fraudulento y engañoso, la propuesta de Reglamento de la Comisión sobre cooperación en materia de protección de los consumidores prevé también la cooperación con los terceros países en el ámbito de la imposición de las normas. La Organización de Cooperación y Desarrollo Económicos (OCDE) adoptó en 2003 una recomendación destinada a proteger a los consumidores contra las prácticas comerciales transfronterizas fraudulentas y engañosas[32].

[32] OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, OECD, 2003.

3.5.2. Acciones propuestas

A nivel multilateral, algunos Estados miembros participan ya activamente en foros como la OCDE, donde se trabaja sobre el *spam*. Se insta a participar activamente en estos trabajos, en particular con vistas a la elaboración de soluciones a nivel internacional.

La Comisión acogerá, en febrero de 2004, un seminario de la OCDE sobre el *spam* con el que se intentará comprender mejor los problemas que plantea y contribuir a la elaboración de soluciones a nivel internacional. Se diseñarán acciones de seguimiento concretas a nivel de la OCDE sobre la base de los resultados del seminario. Los servicios de la Comisión examinan actualmente estas posibles acciones con los Estados miembros, teniendo presentes los trabajos de la OCDE para promover la eficacia de la legislación a nivel internacional, la sensibilización, las soluciones técnicas, la autorregulación y la cooperación internacional en el ámbito de las medidas para hacer cumplir la normativa.

Por lo que se refiere a las Naciones Unidas, la Declaración de la Cumbre Mundial sobre la Sociedad de la Información (Ginebra, 10-12 de diciembre de 2003) y el plan de acción asociado subrayan la necesidad de abordar el *spam* a los niveles nacionales e internacionales convenientes. La Comisión determinará cuál es la mejor manera de reflejar los resultados de la Cumbre Mundial en la UE, teniendo presente la Cumbre de Túnez que tendrá lugar en 2005.

Se invita también a los Estados miembros y las autoridades competentes a reforzar, o establecer si no existe aún, la cooperación bilateral con terceros países. Eso incluye no sólo la promoción de una legislación eficaz, sino también la cooperación en materia de cumplimiento, incluida la cooperación policial y judicial cuando proceda.

Debe impulsarse también la cooperación entre las autoridades y el sector privado, en particular ISP y ESP, para poder rastrear a los remitentes del *spam*, a reserva de las garantías jurídicas apropiadas.

Los servicios de la Comisión seguirán participando activamente en los foros internacionales, incluidos la OCDE y el seminario que la Comisión acogerá en Bruselas en febrero de 2004. Seguirán asimismo organizando reuniones y debates bilaterales con terceros países, en particular para instarles a adoptar medidas eficaces contra el *spam*, especialmente contra sus formas más desagradables, y a promover la cooperación en materia de imposición.

Los servicios de la Comisión han comenzado a examinar, con ayuda de los Estados miembros y las autoridades nacionales interesadas, el mejor medio de garantizar la cooperación internacional, en particular por lo que se refiere a la tramitación de las denuncias relativas al *spam* procedente de terceros países. Este trabajo conjunto con las autoridades nacionales continuará a lo largo de 2004.

3.6. Seguimiento

3.6.1. Análisis

Con el fin de evaluar el funcionamiento práctico del sistema de consentimiento previo y de combatir problemas concretos con las medidas adecuadas, los Estados miembros necesitarán información objetiva y actualizada sobre las tendencias en materia de *spam*,

denuncias de los usuarios y dificultades encontradas por los proveedores de servicios. Las fuentes y el tipo de información necesaria a tal efecto incluirían: tendencias en cuanto a la naturaleza de *spam*, origen y volumen de correo electrónico comercial no solicitado detectado por los proveedores de programas de filtrado, los proveedores de servicios y las iniciativas (reguladoras) nacionales, así como, cuando proceda, las estadísticas de los buzones electrónicos de denuncias.

La OCDE trabaja desde 2003 en la medición de los mensajes electrónicos no solicitados a nivel internacional y proseguirá esta actividad en 2004.

El artículo 18 de la Directiva sobre la intimidad y las comunicaciones electrónicas prevé, para 2006, la presentación de un informe sobre la aplicación de la Directiva y su impacto en los agentes económicos y los consumidores, haciendo especial hincapié en las comunicaciones no solicitadas. Para elaborar este informe, la Comisión deberá obtener información, en particular de tipo estadístico, de los Estados miembros.

3.6.2. Acciones propuestas

Los Estados miembros deberían asegurarse de que disponen de la información y las estadísticas necesarias para orientar sus esfuerzos para hacer cumplir la normativa, cuando proceda en cooperación con la industria y teniendo en cuenta los trabajos que está realizando la OCDE sobre la medición de los mensajes electrónicos no solicitados.

La Comisión recurrirá al Grupo informal en línea sobre las comunicaciones comerciales no solicitadas creado recientemente para facilitar y coordinar los intercambios de información y mejores prácticas sobre las tendencias y estadísticas en materia de *spam*.

4. ACCIONES TÉCNICAS Y DE AUTORREGULACIÓN PARA LA INDUSTRIA

La presente sección, relativa a la autorregulación y a las cuestiones técnicas, incluye medidas que se refieren especialmente a los agentes del mercado, en ámbitos tales como las disposiciones contractuales, los códigos de conducta, las prácticas de comercialización aceptables, las etiquetas o los mecanismos alternativos de solución de litigios, junto con algunas soluciones técnicas como el filtrado y la seguridad de los servidores.

4.1. Aplicación efectiva del régimen de consentimiento previo

4.1.1. Análisis

La lucha contra el *spam* atañe a todas las partes interesadas. La industria puede desempeñar un papel específico al respecto, convirtiendo el régimen de consentimiento previo en una práctica comercial cotidiana. Esta práctica incluye no sólo las condiciones aplicadas a los usuarios finales, sino también las transacciones con los socios comerciales.

En muchos casos, conviene garantizar una coordinación más estrecha a través de las asociaciones profesionales y una mayor participación de los órganos de autorregulación sectoriales y de las asociaciones de consumidores/usuarios, así como de las autoridades responsables de la protección de datos u otras autoridades nacionales competentes.

Mejores prácticas

A título de ejemplo, la «Plataforma de Comercio Electrónico» de los Países Bajos alberga desde 2002 una plataforma consagrada a los principios fundamentales del correo electrónico comercial, que reúne a distintas ramas del sector (venta directa e ISP) y a la asociación holandesa de consumidores. Esta iniciativa tiene por objetivo desarrollar la aplicación práctica del principio de consentimiento previo. Esta aplicación práctica será sometida a prueba con la autoridad responsable de la protección de datos[33].

Los contratos pueden contribuir a la lucha contra el *spam* si incorporan cláusulas de salvaguardia que protejan los derechos individuales. Un gran número de proveedores de servicios de Internet (ISP) y de proveedores de servicios de correo electrónico (ESP) incluyen ya en los contratos con sus clientes la obligación de no utilizar sus servicios para el envío de *spam*. Estos ISP y ESP prohíben el envío de correo electrónico no solicitado o la distribución masiva de correo electrónico desde sus cuentas de correo electrónico[34].

Es muy probable que los conceptos utilizados en los contratos celebrados hasta ahora por los ISP y sus clientes sean diferentes de los utilizados en la nueva Directiva y en la legislación nacional que la incorpore al Derecho interno.

En términos de servicio al cliente, es importante también adoptar una política de filtrado más voluntarista facilitando información sobre los filtros *antispam* y proponiendo en opción a los abonados servicios o dispositivos de filtrado.

Lo mismo sucede cuando los ISP o los operadores de redes móviles firman contratos con terceros, y, en particular, con empresas de venta directa. Esto afecta, por ejemplo, no sólo a las relaciones directas con las empresas que proponen servicios de «valor añadido», sino también a los operadores con los que un proveedor de servicios dado tiene acuerdos de interconexión, como es el caso de los servicios móviles.

El nuevo régimen de consentimiento previo tiene también repercusiones sobre varias actividades de venta directa, como:

- los métodos utilizados para recoger direcciones de correo electrónico y otros datos de acuerdo con el nuevo régimen (como ya se ha dicho, la recolección de direcciones de correo electrónico es incompatible con el Derecho comunitario);

- la adaptación de las listas existentes;

- las prohibiciones que pesan sobre la utilización no autorizada de los datos y la venta de listas no conformes a la normativa.

---

33 Véase http://www.ecp.nl/projecten.php#32.

34 Estas cláusulas se basan a veces en la necesidad de adoptar todas las medidas necesarias para prevenir el uso inadecuado de sus servicios. En otros casos, se remiten a códigos de conducta existentes relativos a la distribución masiva de correo electrónico o a principios de autorregulación (p. ej., «Netiquette»).

4.1.2. Acciones propuestas

Conviene promover la participación de la industria y la autorregulación, o incluso la corregulación, en particular, en los ámbitos donde la legislación y las medidas coercitivas de las autoridades públicas pudieran revelarse insuficientes. Todas las partes interesadas deben desempeñar el papel que les corresponde, incluidas las asociaciones de consumidores y/o de usuarios.

Prácticas contractuales de los proveedores de servicios hacia sus abonados y socios comerciales

En primer lugar, la industria deberá en particular evaluar la conformidad de los contratos existentes con las nuevas disposiciones y proceder, en su caso, a las adaptaciones pertinentes.

Deberán adaptarse las condiciones de los contratos de abono. Esto es aplicable no sólo a los ISP y ESP, sino también a los proveedores de servicios móviles. Con carácter complementario, podría ofrecerse a los clientes información sobre filtros y programas o servicios de filtrado opcionales (sobre el filtrado, véase también el punto 4.3). Las cláusulas que figuran en los contratos firmados con los socios comerciales (en el caso, p. ej., de la interconexión móvil y los servicios de valor añadido) deberían reflejar igualmente unas prácticas comerciales conformes al régimen de consentimiento previo y prever sanciones adecuadas en caso de incumplimiento.

Prácticas de las empresas de venta directa

En segundo lugar, podría resultar necesaria la adaptación de las prácticas de las empresas de venta directa al régimen de consentimiento previo. Podrían, en particular, ponerse de acuerdo sobre métodos específicos conformes a la legislación de recogida de datos personales (como los sistemas de consentimiento «doble» o «confirmado»).

Códigos de conducta

En tercer lugar, las asociaciones sectoriales han anunciado ya distintas iniciativas, como la adaptación o la aprobación de códigos de conducta y la difusión de buenas prácticas de comercialización[35]. La Comisión apoyará la elaboración de códigos de conducta en línea a escala europea en el ámbito de la venta directa. Dichos códigos, al igual que cualquier otra iniciativa de autorregulación y que los contratos, deben ajustarse a las normas del régimen de consentimiento previo. La participación de la autoridad reguladora competente podría ser útil a este respecto. Conviene recordar en este contexto que el Grupo de trabajo sobre protección de datos del artículo 29 puede aprobar códigos de conducta de alcance comunitario (véase el artículo 30 de la Directiva «general» sobre protección de datos, 95/46/CE).

Como ocurre a menudo, la aplicación efectiva de las soluciones basadas en la autorregulación dependerá de la estructura que se establezca para controlar la conformidad con las normas convenidas, y en particular de la eficacia de las sanciones previstas.

[35] La European Federation of Direct Marketing (FEDMA) ha anunciado la publicación en línea de un código de conducta para las empresas de venta directa.

Etiquetas

En cuarto lugar, con vistas a la sensibilización de los usuarios, podrían utilizarse instrumentos tales como etiquetas (p. ej., las denominadas «marcas de confianza» o «sellos web»), en particular cuando el respeto de los códigos de conducta por los agentes del mercado sea supervisado y certificado por terceros de confianza.

La presencia de etiquetas visibles puede ayudar a los usuarios a determinar cuáles son los ISP, los ESP y otros agentes industriales que siguen las normas de la UE y/o los códigos de conducta reconocidos que las aplican. Estas etiquetas podrían también contribuir a reforzar la eficiencia de los sistemas de filtrado.

Podría establecerse el etiquetado de las bases de datos de usuarios y de los mensajes electrónicos que respetasen el régimen de consentimiento previo (p. ej., aplicación de la etiqueta «ADV» en el «asunto» de un mensaje electrónico para indicar que contiene publicidad).

Las etiquetas podrían también permitir a los destinatarios identificar claramente estas comunicaciones comerciales de conformidad con la Directiva sobre comercio electrónico (véase la letra a) del artículo 6 de la Directiva 2000/31/CE, así como la sección 2 del presente documento).

4.2. Mecanismos alternativos de solución de litigios (ADR)

4.2.1. Análisis

En el caso de violaciones de la intimidad tales como el envío de correo electrónico no solicitado, la instauración de un mecanismo extrajudicial de solución de litigios podría contribuir a un mayor respeto de las nuevas normas. Se han puesto en marcha distintas iniciativas a nivel nacional y de la UE con el fin de crear mecanismos sustitutivos de solución de los litigios (ADR) relacionados con las transacciones y comunicaciones en línea. La Comisión adoptó en 1998 y en 2001 recomendaciones relativas al ADR en las que se establecen los principios aplicables a estos sistemas. Están en marcha varias iniciativas en el ámbito de los sistemas de ADR orientados hacia la protección de los consumidores (p. ej., EEJ-NET)[36]. El artículo 17 de la Directiva sobre el comercio electrónico fomenta también la creación de tales mecanismos.

En algunos países existen mecanismos extrajudiciales de solución de litigios, creados a veces por la legislación, pero que difieren unos de otros por numerosos conceptos: origen (mecanismos sectoriales, p. ej. para la venta directa o la comercialización por correo electrónico), «jurisdicción», competencias y sanciones (p. ej., daños y perjuicios), participación de determinadas autoridades (p. ej., las APD, los organismos de deontología publicitaria), etc.

Para ser eficaces, estos mecanismos deben cumplir algunas condiciones relativas, en particular, a su organización y promoción, así como a las medidas previstas para garantizar la ejecución de lo decidido. Su instauración exigiría también la cooperación entre las autoridades y la industria.

---

[36] Más información en: http://europa.eu.int/comm/consumers/redress/out_of_court/index_en.htm.

4.2.2. Acciones propuestas

Se propone instaurar, sobre la base de las iniciativas existentes (como EEJ-NET) si es posible, mecanismos eficaces de denuncia basados en la autorregulación y mecanismos alternativos de solución de litigios (ADR). La creación de tales mecanismos podría resultar especialmente útil cuando fuera difícil conseguir la cooperación internacional.

4.3. Cuestiones técnicas

4.3.1. Análisis

Son varias las soluciones utilizadas para luchar contra el *spam* por medios técnicos. La comunidad de Internet (p. ej., RIPE, IETF) ha tomado también muy en serio el problema del *spam*[37]. Las iniciativas a plazo más largo, como las nuevas normas técnicas aplicables al correo electrónico, no están cubiertas en el presente documento. Los ISP y los ESP bloquean a menudo los mensajes procedentes de servidores utilizados para el envío de *spam* (listas negras) hasta que se identifica la fuente del *spam* y se le impide la utilización del servidor. Además, los usuarios pueden emplear programas de filtrado en su propio equipo terminal y los prestadores de servicios de comunicaciones electrónicas en sus servidores.

No obstante, todas las prácticas y técnicas de filtrado no ofrecen el mismo grado de control al usuario, ni tampoco las mismas garantías en términos de protección de los datos y de la intimidad, tales como el respeto de la confidencialidad de las comunicaciones. Puede ser, asimismo, que aún no se ajusten al nuevo régimen de consentimiento previo aplicable a las comunicaciones comerciales en los países de la UE (consentimiento previo, relación con la comercialización, distribución masiva e individual). Además el establecimiento de una distinción más clara entre la comercialización legal (p. ej., las prácticas conformes al régimen de consentimiento previo) y las comunicaciones comerciales no solicitadas podría permitir el desarrollo de programas de filtrado más eficaces.

Si es cierto que las nuevas disposiciones jurídicas sobre el correo electrónico comercial no solicitado ofrecen garantías suplementarias para el usuario y una mejor base a los proveedores de servicios para adoptar cuando se les pida medidas contra los remitentes de *spam*, también puede suceder que los dispositivos de filtrado bloqueen correo electrónico legítimo (los «falsos positivos») o dejen pasar el *spam* («falsos negativos»). En algunos casos, podría ocurrir que el remitente o el destinatario previsto emprendiera acciones judiciales contra un ISP/ESP. Por este motivo, algunos ISP/ESP proponen a sus usuarios un servicio de filtrado como opción y solicitan su autorización para activarlo.

---

[37] Así por ejemplo, el Grupo de trabajo de lucha contra el *spam* de RIPE (Réseaux IP Européens) lleva a cabo sus actividades desde 1998 (el documento «Good Practice for combating Unsolicited Bulk Email» es accesible en el sitio web de RIPE http://www.ripe.net). Más recientemente, el IRTF (Internet Research Task Force) ha creado un Grupo de investigación sobre la lucha contra el *spam* (véase: http://www.irtf.org/charters/asrg.html). Este grupo podría desarrollar ciertas tecnologías que sirvieran de punto de partida de los trabajos de normalización dentro del IETF (Internet Engineering Task Force).

El recurso a técnicas de filtrado para luchar contra el *spam* plantea también otros problemas, como las relaciones entre el filtrado y la libertad de expresión y entre el filtrado y la obligación contractual que tienen los ISP/ESP de transmitir mensajes de correo electrónico a los clientes de sus clientes, pero estas cuestiones quedan fuera del alcance de la presente Comunicación.

En los servicios móviles, dado que el modelo comercial es distinto del de los servicios de Internet fijos, podrían estudiarse soluciones diferentes para el filtrado. En este modelo suelen aplicarse gastos de entrega por mensaje que hacen más costoso el *spam*. Sin embargo, algunos servicios nuevos implican una facturación basada en la recuperación, lo que significa que el *spam* aumenta los costes para el destinatario. Además, es posible ya entregar correo electrónico en los terminales móviles. Por tanto, se podrían facilitar a los abonados filtros y recursos de visualización para administrar el *spam* móvil.

Es necesario prestar también una atención especial a los servidores en modo abierto (*open relay*). Se trata de servidores SMTP que pueden utilizarse para retransmitir mensajes enviados por usuarios que no son los usuarios locales del servidor. En el pasado, la mayoría de los servidores eran de este tipo. Sin embargo, estos servidores pueden ser utilizados por los remitentes de *spam* para enviar comunicaciones no solicitadas con gran facilidad. Podrían reducirse las posibilidades de uso indebido en este ámbito mediante sencillas medidas preventivas. Lo mismo cabe decir de los proxy abiertos, que son servidores en los que se ejecutan programas que permiten una interacción directa con Internet.

4.3.2. Acciones propuestas

Se invita a los Estados miembros y a las autoridades competentes a clarificar las condiciones jurídicas de funcionamiento de los distintos tipos de programas de filtrado en el país en cuestión, con inclusión de los requisitos relacionados con la intimidad.

Los proveedores de programas de filtrado deben velar por que sus sistemas de filtrado sean compatibles con el régimen de consentimiento previo y demás prescripciones del Derecho de la UE, incluidas las vinculadas a la confidencialidad de las comunicaciones.

Los usuarios deberían tener la posibilidad de decidir qué suerte debe correr el *spam* entrante, en función de sus necesidades. Los proveedores de programas de filtrado deben tener en cuenta las consecuencias para los usuarios de los «falsos positivos», los «falsos negativos», determinadas formas de filtrado basado en el contenido y los posibles problemas de responsabilidad asociados.

Las empresas de filtrado deberían cooperar con las partes interesadas para desarrollar técnicas de reconocimiento del correo electrónico comercial que respondan a las prácticas comerciales aceptadas en virtud del Derecho comunitario, incluyendo sellos web, etiquetas, etc.

Los proveedores de servicios de correo electrónico (y de servicios móviles cuando proceda) deberían proponer como opción a sus clientes productos o servicios de filtrado, e informarles acerca de los propuestos por terceros.

Los propietarios de servidores de correo electrónico deberían garantizar la seguridad de sus servidores, de manera que no funcionen en el modo abierto (salvo que esté justificado). Lo mismo cabe decir de los proxy abiertos.

5. ACCIONES DE SENSIBILIZACIÓN

Esta sección relativa a sensibilización incluye las acciones propuestas en ámbitos como la prevención, la sensibilización de los consumidores y la notificación de problemas.

5.1. Análisis

Los Estados miembros de la UE tenían que haber incorporado a su Derecho interno el nuevo régimen de consentimiento previo aplicable al correo electrónico no solicitado a más tardar el 31 de octubre de 2003. Ahora bien, aunque este nuevo enfoque tuvo un amplio eco en la prensa, es posible que subsistan algunas dudas, entre los agentes del mercado y los ciudadanos, sobre el significado del régimen de consentimiento previo en la práctica[38].

Este nuevo enfoque se basa en el derecho del usuario a prestarse o no a recibir comunicaciones comerciales. Para ello, no obstante, el usuario debe conocer las normas básicas aplicables a las comunicaciones no solicitadas y a quién dirigirse si surgen problemas.

Mejores prácticas

El Comisario de Información del Reino Unido (autoridad responsable de la protección de datos en este país) publicó, pocas semanas antes de la entrada en vigor de la nueva normativa por la que se transpone la Directiva, un documento orientativo en el que se explican las nuevas normas, una de cuyas partes estaba dedicada a la comercialización por medios electrónicos. La Comisión de Información anunció también que podrían obtenerse formularios de denuncia tanto en línea como en sus oficinas en cuanto entraran en vigor las normas, explicando qué información se necesitaría probablemente[39].

Los usuarios deben también comprender los riesgos que implica la comunicación de sus datos personales en Internet (p. ej. dejándolos al visitar sitios web o Usenet) y deberían adaptar su comportamiento en consecuencia.

Por último, es necesario que sepan qué tipos de programas de filtrado existen en el mercado y qué pueden hacer por ellos los proveedores de servicios y programas (p. ej., los ISP y ESP).

---

38 Se encontrará información general sobre las normas aplicables a las comunicaciones no solicitadas en virtud de la Directiva 2002/58/CE en la dirección: http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited.

39 Véase: http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_2002/58/EC.html#guidance

Mejores prácticas

La «Commission National Informatique et Libertés» (CNIL), autoridad francesa responsable de la protección de datos, ha puesto en línea en su sitio web una información muy completa sobre distintos aspectos del *spam*: resultados de su campaña «buzón de *spam*» y asuntos sometidos a las autoridades judiciales (véase más abajo), consejos básicos sobre la prevención del *spam*, información sobre la manera de notificarlo, datos sobre las asociaciones de usuarios activas en este ámbito, etc.

Aunque en la mayoría de los Estados miembros ya se han emprendido o están previstas actividades de sensibilización relativas al nuevo régimen de consentimiento previo, difieren ampliamente en cuanto a calendario, naturaleza de la información proporcionada, público destinatario y partes implicadas. Algunos Estados miembros, no obstante, han preferido esperar hasta que su legislación esté lista. Siempre que se han organizado consultas pública sobre la aplicación de la Directiva 2002/58/CE, han contribuido en cierta medida a la sensibilización.

Es posible que sean varias las autoridades (p. ej., las APD, las ANR, las APC, el defensor del pueblo) responsables de estas actividades, en función de sus competencias respectivas en un Estado miembro dado. No existe (aún) coordinación entre las distintas autoridades competentes en todos los Estados miembros. Parece que en algunos están involucrados los Ministerios, y es frecuente la participación de asociaciones sectoriales. A veces, también las asociaciones de consumidores o usuarios participan en estas actividades.

Algunos agentes de la industria han emprendido también actividades de sensibilización a escala nacional, europea o mundial, aunque también en este caso las diferencias pueden ser considerables. Estas actividades incluyen, en particular:

- guías prácticas destinadas a las empresas de venta directa, o campañas específicamente concebidas para el sector de las comunicaciones;
- consejos generales a los clientes sobre los códigos de conducta, los mecanismos de denuncia y el filtrado;
- plataformas/grupos de trabajo encargados de elaborar buenas prácticas para las comunicaciones comerciales.

5.2. Acciones propuestas

Con el fin de que se conozca bien lo que debe y no debe hacerse en materia de correo electrónico comercial, es necesaria a corto plazo una acción de envergadura y sostenida en todos los Estados miembros, referida tanto a la prevención como a la aplicación de las normas. Conviene facilitar información práctica sobre la prevención, las prácticas de comercialización aceptables y las soluciones técnicas y jurídicas con que cuentan los usuarios.

Se invita a todas las partes implicadas, desde los Estados miembros y las autoridades competentes hasta las asociaciones de consumidores y usuarios, pasando por las empresas, a comprometerse en las actividades de sensibilización. Se invita a los Estados miembros y las autoridades competentes que aún no lo hayan hecho a iniciar campañas de sensibilización a principios de 2004 o a apoyarlas.

Por lo que se refiere en particular a la naturaleza de la información facilitada, las actividades destinadas a las empresas y/o a los consumidores deberían incluir:

– explicaciones básicas, pero globales, sobre las nuevas normas y los derechos de las empresas y/o los consumidores en virtud de ellas;

– información práctica sobre las prácticas de comercialización aceptables en el marco del régimen de consentimiento previo, clarificando, en particular, el concepto de recogida legítima de datos personales;

– información práctica para que los consumidores sepan cómo evitar el *spam* (por ej. utilización de los datos personales, etc.);

– información práctica para los consumidores sobre productos y servicios disponibles para evitar el *spam* (p. ej., filtrado, seguridad);

– información sobre las medidas prácticas que deben adoptarse en caso de recibir *spam*, incluidos los mecanismos de denuncia y los sistemas ADR si existen.

El programa sobre la seguridad de Internet y el *spam*

La Comisión Europea ha publicado una convocatoria de propuestas dentro de este programa que admite proyectos de lucha contra el *spam* en varias acciones, p. ej. sobre sensibilización. Los proyectos seleccionados en la primera evaluación de la convocatoria podrían iniciarse en mayo de 2004.

La Comisión prepara actualmente una propuesta de programa continuador que prevé la financiación de nuevas medidas para combatir los contenidos ilícitos, nocivos e indeseados, como el *spam*.

http://www.europa.eu.int/information_society/programmes/iap/call/index_en.htm

Estas acciones deberían estar orientadas a los siguientes grupos:
a) empresas implicadas en la venta directa o que la utilizan,
b) consumidores abonados a servicios de correo electrónico, incluidos los servicios SMS,
c) proveedores de servicios de correo electrónico, incluidos los proveedores de servicios móviles.

Las actividades de sensibilización deberían ser realizadas por distintos canales (no solamente a través de la Red), para llegar realmente a los distintos destinatarios previstos. La participación de las asociaciones sectoriales y de consumidores adquiere gran importancia en este contexto. Conviene garantizar la coordinación de las distintas iniciativas posibles.

Las acciones mencionadas anteriormente deberían también hacer referencia a los códigos de conducta del sector eficaces, a los mecanismos de denuncia, a las etiquetas (p. ej., marcas de confianza) y a los sistemas de certificación eventualmente disponibles.

Los servicios de la Comisión facilitan ya información sobre lo fundamental del régimen de consentimiento previo en el sitio web EUROPA[40].

Remitirán también, mediante hiperenlaces, a los aspectos nacionales de la aplicación así como a las cifras y tendencias básicas en materia de *spam* cuando se disponga de ellas.

[40] http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/*spam*/index_en.htm

Los servicios de la Comisión recurrirán también a los centros europeos de información empresarial para difundir información sobre las nuevas normas.

CONCLUSIÓN

El *spam* es uno de los retos principales a que se enfrenta actualmente Internet. Será necesario, para luchar contra este fenómeno, actuar en distintos frentes, propiciando no sólo una aplicación eficaz de las normas y la cooperación internacional, sino también las soluciones de autorregulación y técnicas por parte de la industria, así como la sensibilización de los consumidores. El cuadro siguiente contiene una síntesis de las acciones enumeradas en la presente Comunicación.

La Comisión apoyará desde luego estos esfuerzos cuanto le sea posible, pero corresponderá sobre todo a los Estados miembros de la UE y a sus autoridades competentes, al sector y a los consumidores y usuarios de Internet y de los servicios de comunicaciones electrónicas desempeñar el papel que les corresponde a nivel nacional e internacional.

Una aplicación integrada y en paralelo del conjunto de acciones enumeradas en la presente Comunicación, contando con un amplio apoyo de las partes interesadas, puede contribuir a reducir considerablemente el volumen de *spam* que actualmente contrarresta las ventajas que el correo electrónico y otros medios de comunicación electrónica aportan a nuestras sociedades y nuestras economías.

La Comisión efectuará un seguimiento de la aplicación de estas acciones en 2004, en particular a través del Grupo informal sobre comunicaciones no solicitadas, y evaluará, a más tardar para finales de 2004, si hacen falta medidas suplementarias o correctivas.

CUADRO: RESUMEN DE LA SERIE DE ACCIONES ENUMERADAS EN LA COMUNICACIÓN

En el cuadro siguiente se recapitulan las acciones enumeradas en la Comunicación. Las que dependen de la Comisión o de los servicios de la Comisión figuran separadamente. Como ya se ha indicado, las acciones guardan diversas relaciones entre sí y deberían aplicarse, en la medida de lo posible, en paralelo y de manera integrada.

I – Aplicación efectiva y control de esta aplicación por los Estados miembros y sus autoridades competentes

Como condición previa, los Estados miembros deben transponer sin más demora la Directiva sobre la intimidad y las comunicaciones electrónicas, y en particular las disposiciones relativas a las comunicaciones no solicitadas.

Los Estados miembros y las autoridades competentes deben evaluar la eficacia de sus mecanismos para hacer cumplir la normativa (recursos y sanciones, mecanismos de denuncia, cooperación interna en la UE y cooperación con terceros países y seguimiento). Los Estados miembros deben también elaborar estrategias nacionales con el fin de garantizar la cooperación entre las APD, las APC y las ANR, y evitar el solapamiento de competencias y la duplicación de esfuerzos entre las distintas autoridades.

Los Estados miembros y las autoridades competentes deben, en particular:

a) Recursos y sanciones eficaces

- ofrecer a las víctimas posibilidades adecuadas para reclamar daños y perjuicios y prever sanciones eficaces, incluidas las de tipo económico y las penales cuando proceda;

- en los Estados miembros que no disponen de vías de recurso administrativo, prever la creación de tales vías a fin de hacer aplicar las nuevas normas;

- dotar a las autoridades competentes de las facultades de investigación y ejecución necesarias.

b) Mecanismos de denuncia

- establecer mecanismos de denuncia adecuados, incluidos buzones electrónicos que recojan las denuncias de los usuarios;

- coordinar la actuación de las distintas autoridades nacionales competentes.

c) Denuncias transfronterizas y cooperación en materia decumplimiento dentro de la UE

- utilizar un mecanismo de enlace ya existente (o crearlo si es preciso) para que las autoridades nacionales puedan cooperar con el fin de hacer aplicar las normas a escala transfronteriza en el territorio de la UE (intercambio de información, asistencia mutua). En este marco, por lo que se refiere en particular al *spam* fraudulento y engañoso, se invita al Consejo y el Parlamento a aprobar lo más rápidamente posible la propuesta de Reglamento relativo a la cooperación en materia de protección de los consumidores y a examinar en qué medida debe añadirse la Directiva sobre la intimidad y las comunicaciones electrónicas al ámbito de aplicación de dicho Reglamento.

d) Cooperación con terceros países

- participar activamente en los foros multilaterales (por ejemplo la OCDE) con el fin de elaborar soluciones a nivel internacional;

- reforzar, o en su caso iniciar, la cooperación bilateral con los terceros países;

- estudiar, con la Comisión, qué iniciativa específica podría adoptar ésta para facilitar la cooperación internacional;

- cooperar con el sector privado con el fin de detectar los remitentes de *spam*, a reserva de las garantías jurídicas apropiadas.

e) Seguimiento

- asegurarse de que disponen de la información y las estadísticas requeridas para hacer cumplir la normativa, en cooperación con la industria cuando proceda, y teniendo en cuenta los trabajos sobre medición que lleva a cabo actualmente la OCDE.

II – Acciones técnicas y de autorregulación por parte del sector

Los agentes del mercado (p. ej., los ISP, los ESP, los operadores de redes móviles, las empresas de software, las empresas de venta directa) deben convertir el régimen de consentimiento previo en una práctica cotidiana, en cooperación con las asociaciones de consumidores y usuarios y las autoridades competentes cuando proceda, y en particular:

a) Acciones de autorregulación

- evaluar, y si es preciso adaptar, las prácticas contractuales de los proveedores de servicios (ISP, ESP, operadores móviles) en relación con sus abonados y sus socios comerciales; facilitar información sobre el filtrado y suministrar quizás opcionalmente a los clientes programas o servicios de filtrado;

- adaptar las prácticas de venta directa al régimen de consentimiento previo y ponerse eventualmente de acuerdo sobre métodos concretos de recogida de datos personales conformes al Derecho (p. ej., sistemas de consentimiento «doble» o «confirmado»);

- elaborar y difundir códigos de buenas prácticas eficaces (p. ej., la iniciativa FEDMA) conformes al régimen de consentimiento previo, en cooperación con el Grupo de trabajo sobre protección de datos del artículo 29 o con las autoridades nacionales competentes cuando proceda;

- estudiar la posible utilización de etiquetas para los mensajes electrónicos que respetan el régimen de consentimiento previo y de bases de datos para ayudar a los usuarios (y a los filtros) a reconocerlos, de conformidad con la Directiva sobre comercio electrónico;

- utilizar, o crear si es necesario, mecanismos de denuncia y mecanismos alternativos de solución de litigios (ADR) en el marco de la autorregulación, que sean eficaces y se basen en iniciativas existentes en la medida de lo posible (p. ej., EEJ-NET).

b) Acciones técnicas

- (Los proveedores de programas de filtrado) deben velar por que sus sistemas de filtrado sean compatibles con el régimen de consentimiento previo y demás exigencias del Derecho de la UE, incluidas los vinculadas a la confidencialidad de las comunicaciones. Se invita a los Estados miembros y a las autoridades competentes a clarificar las condiciones jurídicas para el funcionamiento de los distintos tipos de programas de filtrado en el país en cuestión, y en particular los requisitos relacionados con el respeto de la intimidad.

- (Los proveedores de programas de filtrado) deben tener en cuenta las consecuencias para los usuarios de los «falsos positivos», los «falsos negativos» y determinadas formas de filtrado basado en los contenidos, así como de los posibles problemas de responsabilidad asociados. Los usuarios deben tener la posibilidad de decidir qué se hace con el *spam* entrante, en función de sus necesidades.

- (Los proveedores de programas de filtrado) deben cooperar con las partes interesadas para desarrollar técnicas de reconocimiento de los mensajes comerciales legítimos (es decir, que corresponden a las prácticas comerciales aceptadas en virtud del Derecho comunitario), utilizando por ejemplo etiquetas.

- (Los proveedores de servicios de correo electrónico, y de servicios móviles cuando proceda) deben ofrecer en opción productos o servicios de filtrado a los clientes que lo soliciten, e informarlos sobre los propuestos por terceros.

- (Los propietarios de servidores de correo electrónico) deberían garantizar la seguridad de sus servidores, de manera que no funcionen en el modo abierto (salvo que esté justificado). Lo mismo cabe decir de los proxy abiertos.

III – Acciones de sensibilización por parte de los Estados miembros, el sector y las asociaciones de consumidores o usuarios

Se invita a los Estados miembros y las autoridades competentes que aún no lo hayan hecho a iniciar campañas de sensibilización a principios de 2004 o a apoyarlas. Todas las partes implicadas, desde los Estados miembros y las autoridades competentes hasta las asociaciones de consumidores y usuarios, pasando por las empresas, deberían participar en las campañas de información práctica en materia de prevención, prácticas de comercialización aceptables y soluciones técnicas y jurídicas a disposición de los usuarios, y en particular:

- orientar las acciones hacia a) empresas implicadas en la venta directa o que la utilizan, b) consumidores abonados a servicios de correo electrónico, incluidos los servicios SMS, y c) proveedores de servicios de correo electrónico, incluidos los proveedores de servicios móviles.

- facilitar a las empresas y/o a los consumidores:

- explicaciones básicas, pero globales, sobre las nuevas normas y sus derechos en virtud de ellas;

- información práctica sobre las prácticas de comercialización aceptables en el marco del régimen de consentimiento previo, clarificando, en particular, el concepto de recogida legítima de datos personales;

- información práctica para que los consumidores sepan cómo evitar el *spam* (por ej. utilización de los datos personales, etc.);

- información práctica para los consumidores sobre productos y servicios disponibles para evitar el *spam* (p. ej., filtrado, seguridad);

- información sobre las medidas prácticas que deben adoptarse en caso de recibir *spam*, incluidos los mecanismos de denuncia y los sistemas ADR si existen;

- referencia a los códigos de conducta del sector eficaces, a los mecanismos de denuncia, a las etiquetas (p. ej., marcas de confianza) y a los sistemas de certificación eventualmente disponibles;

- realización de estas actividades de sensibilización por distintos canales, en línea y fuera de línea, para llegar realmente a los distintos destinatarios previstos.

La participación de las asociaciones sectoriales y de consumidores adquiere gran importancia en este contexto. Conviene garantizar la coordinación de las distintas iniciativas posibles.

IV – Acciones que deben aplicar la Comisión o sus servicios

La Comisión efectuará un seguimiento de la aplicación de las acciones resumidas en 2004, en particular a través del Grupo informal sobre comunicaciones no solicitadas, y evaluará, a más tardar para finales de 2004, si hacen falta medidas suplementarias o correctivas.

En términos generales, la Comisión seguirá supervisando atentamente la aplicación de la Directiva. Procurará, en particular, comprobar que las medidas de transposición nacionales prevén sanciones reales, incluidas las de tipo económico o penal, en caso de violación de las exigencias correspondientes (la Comisión inició en noviembre de 2003 procedimientos de infracción contra varios Estados miembros por ausencia de notificación de sus medidas de transposición nacionales). Los servicios de la Comisión están dispuestos a ayudar a los Estados miembros si resulta necesario.

Los servicios de la Comisión han creado un «Grupo informal en línea sobre comunicaciones comerciales no solicitadas», con el apoyo de los Estados miembros y las autoridades encargadas de la protección de datos. Este Grupo facilitará el trabajo sobre la aplicación efectiva de la Directiva (p. ej., en cuanto a denuncias, recursos, sanciones o cooperación internacional), así como las otras acciones enumeradas en la presente Comunicación.

Los servicios de la Comisión pedirán al Grupo de trabajo sobre protección de datos del artículo 29 que apruebe cuanto antes un dictamen sobre algunos conceptos utilizados en la Directiva de la intimidad y las comunicaciones electrónicas, con el fin de contribuir a una aplicación uniforme de las medidas nacionales adoptadas en virtud de la Directiva.

Los servicios de la Comisión han comenzado a estudiar, con los Estados miembros y las autoridades nacionales encargadas de la imposición, los mejores medios de garantizar la aplicación transfronteriza en el territorio de la UE, así como con los terceros países. Este trabajo continuará a lo largo del año 2004.

La Comisión apoyará los códigos de conducta en línea de alcance europeo para la venta directa, y cuando proceda su aprobación por el Grupo de trabajo sobre protección de datos del artículo 29.

La Comisión acogerá un seminario de la OCDE sobre el *spam* en febrero de 2004 y examinará con los Estados miembros las acciones de seguimiento pertinentes, incluidos los trabajos de la OCDE para promover una legislación eficaz al nivel internacional, la sensibilización, las soluciones técnicas, la autorregulación y la cooperación internacional en materia de imposición.

La Comisión procurará determinar los mejores medios de dar continuidad a los resultados de la Cumbre Mundial sobre la Sociedad de la Información de 2003 en la UE, teniendo en cuenta que en 2005 tendrá lugar la Cumbre de Túnez.

La Comisión ha publicado una convocatoria de propuestas en el marco del programa sobre la seguridad de Internet que permite proponer proyectos de lucha contra el *spam* en varias acciones; la Comisión prepara actualmente una propuesta de programa continuador que propondrá financiar nuevas medidas, en particular para luchar contra el *spam*.

Los servicios de la Comisión seguirán facilitando información sobre las bases del régimen de consentimiento previo en el sitio web EUROPA. Remitirán también, mediante hiperenlaces, a los aspectos nacionales de la aplicación así como a las cifras y tendencias básicas en materia de *spam* cuando se disponga de ellas. Los servicios de la Comisión recurrirán también a los centros europeos de información empresarial para difundir información sobre las nuevas normas.