

CONVERGENCIA EN LOS MODELOS DE REGULACIÓN DEL CORREO ELECTRÓNICO NO SOLICITADO (*SPAMMING*)

Daniel Peña Valenzuela

INTRODUCCIÓN

El correo electrónico no solicitado (*spamming*) se ha convertido en el mayor obstáculo para el pleno desarrollo del mercadeo en línea de productos y servicios. La mayor parte de usuarios y suscriptores con acceso a la red global experimenta molestia, demora y mayores costos, por el tráfico excesivo de mensajes de datos que contienen información inútil o superflua para los consumidores.

Como en general en el caso del internet, la principal pregunta que surge con el correo no solicitado es acerca de la forma más adecuada de regularlo. Al lado de la regulación “técnica” y la “social” aparece el ordenamiento jurídico como la forma de “disciplina” por excelencia de las herramientas técnicas, para que éstas cumplan adecuadamente su función. El carácter civil o penal de la represión al correo electrónico no solicitado y la necesidad de un modelo de regulación más convergente y universal que responda a esas mismas características del correo no deseado son evidentes.

El presente ensayo pretende evaluar las distintas formas de regulación del *spamming* en el contexto internacional, desde la óptica de su implementación y desarrollo, así como un planteamiento de argumentos a favor y en contra de las mismas. Lo anterior puede ser útil en el camino de lograr una posible regulación completa y eficaz en Colombia. También es posible que de llegarse a instrumentos internacionales de represión

del correo no solicitado, Colombia deba tener fundamentos para la construcción de una base propia de negociación.

I. DIFICULTADES EN LA CONSTRUCCIÓN DE UN MODELO IMPERANTE DE REPRESIÓN DEL *SPAMMING*

A. Intentos y perspectivas de definición

El correo electrónico es una de las aplicaciones más extendidas de las tecnologías de la información, como vehículo de envío y recepción de mensajes de datos de todo tipo, con toda clase de contenidos, entre individuos y empresas.

El correo electrónico en la mayoría de los casos no tiene costo para los usuarios, diferente al costo del acceso a la red global. A diferencia del correo normal, en el cual los Estados tenían (aún lo tienen en algunos casos) control a través de entidades públicas encargadas del transporte de la correspondencia, el correo electrónico es ofrecido como un servicio por entidades privadas con alcance global.

La posibilidad de enviar gran cantidad de correos electrónicos con un costo mínimo y en algunos casos con anonimato, ha propiciado la utilización de los mensajes de datos como herramientas de publicidad directa de bienes y servicios.

El correo no solicitado es difícil de definir. Sin embargo, desde la óptica de los usuarios, cada mensaje que reciban sin su autorización o que tenga interés, o incluso en algunos casos, que tenga contenido comercial, puede ser considerado como *spamming*¹. Las formas técnicas de llegar a ese resultado son variadas, así como los métodos utilizados para que el receptor no se cerciore del problema².

La arquitectura del control, con servidores, terminales, direcciones IP y demás mecanismos, ha sido sobrepasada

1 BOB SULLIVAN. "Spam wars: How unwanted e-mail is burying the internet", 2003 en MSNBC at [msnbc.com/news/941040.asp].

2 CERT Coordination Center "Spoofed/Forged e-mail en [cert.org/tech_tips/email_spoofing.html].

por el ingenio de los *spammers*, como se conoce a quienes envían correo no solicitado. Al igual que en otros casos de infracción de derechos, la policía especializada en cibercrimitos y las autoridades judiciales persiguen como “gato al ratón” a los individuos que realizan tal conducta.

Para tratar de definir con mayor claridad este fenómeno se deben establecer sus características preponderantes³:

1. *No solicitado*

Esta noción es aceptada como fundamental para efectos de diferenciar un mensaje de datos comercial, normal y aceptado por el receptor. La comunicación es considerada como no solicitada si no existe una relación previa entre el emisor y el receptor del mensaje. También se considera como una comunicación no deseada aquella que el receptor no ha aceptado expresamente recibir. Más aún, en el caso de una expresa comunicación en la que se haya solicitado la remoción de una lista de correo o la decisión de no querer recibir más mensajes, se entendería como la voluntad explícita de considerar el próximo mensaje como no solicitado.

2. *Comercial*

La característica de ser correo “comercial” es fundamental, en particular por la creciente utilización masiva de correos para fines de divulgación de ideas políticas o religiosas. Bien es sabido que este tipo de expresión está amparada por el derecho constitucional en cuanto a los valores sociales supremos, como la libertad de expresión. El *spamming*, en su forma más tradicional al menos, se predica de mensajes con contenido “comercial”.

Como “comercial” podríamos incluir, en Colombia, las actividades mercantiles previstas como tales en el Código

3 W. KHONG. “Spam law for the internet”, 2001 *The Journal of Information, Law and Technology* (JILT) en [e1j.warwick.ac.uk/jilt/01-3/Khong.html].

de Comercio, pero también una definición más amplia comprendería la oferta de bienes y servicios. No obstante, deberá tenerse en cuenta que en algunos casos la ganancia puede obtenerse de manera indirecta, lo cual no indica que deje de existir ánimo de lucro⁴.

3. *Volumen o cantidad de mensajes*

De manera general se considera *spamming* al envío simultáneo de una gran cantidad de mensajes de datos. También se considera como tal el envío de un mensaje a una gran cantidad de receptores. El hecho de que algunas técnicas permitan cierta personalización de los mensajes mediante cambios imperceptibles no afecta la cantidad de mensajes para que exista *spamming*.

Frente a la regulación legal, la definición de cuántos mensajes de datos son necesarios para que se configure el ilícito es una de las dificultades evidentes.

También debe tenerse en cuenta que la recolección de evidencia por parte de los afectados puede ser difícil a la hora de lograr el material probatorio que incluya todos los mensajes enviados por el emisor.

B. Sujetos afectados por el *spamming*⁵

El *spamming* es una consecuencia del aprovechamiento que algunos han hecho de las características del correo electrónico, como su carácter global, la inexistencia de barreras de entrada por el bajo costo de envío masivo de correos y la dificultad de una regulación legal efectiva ante la inexistencia de una jurisdicción global con la aplicación de leyes uniformes.

4 FTC Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Mail, 1998.

5 ADAM MOSSOF. "Spam-Oy, it's such a nuisance!", *Public Law & Legal Theory Working Paper Series*, Research Paper, Michigan State University, 2003.

Desde la óptica de los sujetos damnificados con este problema, existen las afectaciones siguientes:

1. *Los usuarios*

Éstos se afectan desde varios puntos de vista: sus sistemas de información, en particular de sus buzones o bandejas de entrada, son penetrados y ocupados por mensajes de datos no solicitados; la identificación de cuáles mensajes no pertenecen a otros usuarios con los cuales sí existe la voluntad de comunicarse y la posterior eliminación de los mensajes no deseados; los costos por el tiempo de acceso, mayor tiempo de conexión para revisar y borrar los mensajes así como el espacio de memoria –así sea temporal– utilizado en el almacenamiento de los mensajes.

Cada vez con más frecuencia, los usuarios se ven obligados a adquirir programas de computador que sirven para filtrar los mensajes de datos, lo que significa costos extras para individuos y empresarios. Tales herramientas pueden además generar el riesgo de no permitir el ingreso de mensajes que sí se quisieran recibir.

El contenido de los mensajes no solicitados está usualmente asociado a esquemas de fraude, loterías, ventas multinivel, pornografía, ganancia en pirámide, así como a cadenas de cartas fraudulentas. El *spamming* se ha convertido también en una forma “eficiente” de transmisión y difusión de virus y de otras maneras de atacar sistemas de información; es decir, la amenaza creciente del correo electrónico no solicitado está vinculada a atentados contra la seguridad informática.

2. *Proveedores de servicio de internet (PSI)*

Al igual que los usuarios, los proveedores de servicios se afectan de varias maneras por el correo no solicitado. En el tráfico de mensajes de datos, el volumen es fundamental para mantener la eficiencia en la velocidad y en la transmisión; por

esa razón el *spamming* repercute directamente en la reputación del PSI y por ende, en el número de clientes.

La estructura de servicios de la red global es escalonada, en el sentido de que los diversos proveedores de servicios compran capacidad o se interconectan con otros a un costo determinado. De la capacidad existente y de su relación con el tráfico de mensajes de datos depende la eficiencia del PSI y su competitividad frente a otros.

Los principales costos que tienen los PSI en relación con el tráfico de correo electrónico son los administrativos, relativos al manejo y control de la red, y también el almacenamiento.

El aumento inesperado de tráfico puede conllevar la necesidad de inversión en infraestructura para que los PSI puedan mantener el nivel óptimo de servicios en relación con los usuarios.

La importancia del servicio al cliente en los negocios de los PSI, así como la reputación de los mismos, ha llevado consigo que los PSI sean críticos de los esquemas de mercadeo directo que incluyen correo electrónico no solicitado y también hayan combatido este fenómeno en los estrados judiciales.

Todo lo anterior, y en particular el crecimiento exponencial del correo masivo no solicitado, afecta la reputación del propio correo electrónico como herramienta fundamental de comunicaciones privadas y empresariales.

El elemento subjetivo que identifica al emisor de correos masivos se ha desvirtuado paulatinamente, a medida que las regulaciones legales sancionan como ilícita esta conducta. En efecto, las estrategias de quienes envían el correo masivo se han encaminado a usurpar nombres de compañías o personas reconocidas para suplantar esa identidad en el encabezamiento de los correos, lo cual hace más difícil la labor de depuración de las casillas de correo por parte de los usuarios y las herramientas de control de los PSI respecto del tráfico de mensajes de datos.

II. MECANISMOS ACTUALES DE REPRESIÓN DEL CORREO NO SOLICITADO

No existe una solución única y definitiva a los problemas causados por el *spamming*: una combinación de formas de represión y un factor cultural de educación de los usuarios es la actual respuesta. En el caso de los usuarios se debe tener en cuenta que el cuidado de sus direcciones de correo electrónico y sus datos personales es fundamental para la adecuada construcción de la sociedad de la información.

A. Autorregulación

La primera aproximación al correo masivo no solicitado fue derivada de la naturaleza de internet en sus orígenes. El carácter no comercial de la red global tuvo como consecuencia que la reacción a los primeros brotes de correo electrónico no solicitado estuviera vinculada a la acción directa de retaliación y a la exclusión del "grupo social" de quien abusara de las características de los grupos de usuarios de internet y primeros afectados en 1996.

Las reglas de cortesía o etiqueta pronto dieron lugar, con la influencia paulatina de lo comercial en la red global, a códigos y mandatos de autorregulación de las asociaciones y entidades relacionadas con el mercadeo directo.

La importancia de ese tipo de autorregulación no debe menoscabarse. De hecho, existe un consenso internacional en las entidades y asociaciones de mercadeo sobre la proscripción de conductas clasificadas como correo electrónico no solicitado. Por esa razón, estas conductas son actualmente cometidas por individuos y empresas independientes, de poca tradición y en algunos casos vinculadas a actividades fraudulentas.

La autorregulación, sin embargo, no basta para reprimir un fenómeno tan creciente en volumen y con alcance global. Sin una clara determinación de cuáles son los parámetros y

características que configuran *spamming*, es obvio que la mera voluntad de dejar de realizar ese tipo de prácticas puede ser ambigua e ineficiente⁶.

B. Medidas técnicas

Aunque rudimentarias, las principales técnicas de los usuarios están relacionadas con la clasificación que realizan de los mensajes recibidos en cuanto al emisor y al contenido del título.

Esta selección permite que el usuario borre los mensajes que no llenen esas determinadas características (los fabricantes de programas de ordenador de manejo de correo electrónico con frecuencia incluyen en la arquitectura del software los filtros contra correo electrónico no solicitado).

Los filtros se basan en el conocimiento del receptor respecto de los mensajes sospechosos o la probabilidad determinada por unos criterios que definen el rechazo del mensaje. Los filtros pueden tener como base ciertas características relacionadas con el origen del mensaje, por ejemplo, la dirección protocolo-internet o el DNS de proveniencia. Los filtros de contenido predeterminan frases o palabras, las cuales a su vez probablemente significan que el mensaje es no deseado por el receptor.

Los filtros pueden estar ubicados en el servidor –del PSI o del usuario– o en los equipos terminales. Para los PSI, tener los filtros que impidan al mensaje entrar a su sistema de información, facilita el control y reduce los costos adicionales derivados de la administración del exceso de tráfico.

Los proveedores de servicios han establecido esquemas de colaboración entre sí con el fin de elaborar listas de reconocidos emisores de mensajes en bloque. Estas listas facilitan los filtros sin que el usuario final lo note. En relación con el

6 PAUL HOFFMAN. "Unsolicited bulk e-mail: definitions and problems" (Internet Mail Consortium Report: UBE-DEF IMCR-004).

perjuicio causado por el *spamming* a los PSI, se debe tener en cuenta que los costos del bloqueo a veces son transferidos de manera indirecta al usuario, bajo otros conceptos generales como “costos de administración del sistema”. Lo anterior significa que en todo caso el perjuicio sí se causa.

La utilización de filtros por los PSI requiere el previo consentimiento de los usuarios si éstos pueden verse perjudicadas con estos mecanismos tecnológicos, en particular por la pérdida de mensajes que podría afectar a las casillas de los destinatarios. Esto es válido también cuando se utiliza otra herramienta, como la desconexión de la función *relay* en los enrutadores, con el fin de evitar que terceros ajenos al propietario de una dirección la usen para enviar correos masivos no requeridos.

Los *peering agreements*, es decir, los contratos suscritos entre proveedores de servicios, incluyen en algunas ocasiones una regulación específica relacionada con el tráfico de los mensajes que circulen entre los administradores de la red. De esa forma se adjudica la responsabilidad por el tráfico extra y se define contractualmente la colaboración entre las partes respecto de los costos adicionales ocasionados por el *spamming*. De manera indirecta se excluyen así los proveedores de servicios de internet que no tomen medidas adecuadas para combatir este fenómeno.

Las listas de bloqueo del correo electrónico no solicitado son otra posibilidad de lucha contra este flagelo. Se han conformado bases de datos que contienen lista negras o listas de control que son utilizadas por emisores de mensajes de datos sin autorización. Estas listas reciben su nombre de términos en inglés, por ejemplo: *Mail Abuse Prevention System Real Time Black Hole List*, *Relay Spam Stopper*, *Open Relay Behaviour Modification System*, *Dial Up User List Spam Project*. En estas listas se incluyen los sitios y las direcciones más usados por los emisores de correos electrónicos no solicitados, lo que permite a los PSI y a los usuarios saber cuáles de esos recursos deben bloquear o impedir la suscripción a sus servicios.

Tal mezcla de autorregulación y medidas técnicas tiene inconvenientes jurídicos, relacionados con la legitimidad de quienes

elaboran la lista, las condiciones y características que habilitan a los organizadores de la lista para optar por la inclusión.

El caso de la retaliación contra los emisores de mensajes no deseados también debe incluirse en las medidas tecnológicas, por cuanto implica el rastreo de los emisores de *spamming* mediante programas de ordenador específicos y, luego, el envío de mensajes contra el atacante inicial. Estas formas de justicia por los propios medios no deberían ser aceptadas en un entorno como el ciberespacio, que está en búsqueda de legitimidad.

En general, las medidas técnicas reseñadas no atenúan la noción de responsabilidad sino por el contrario son una evidencia del perjuicio económico que el correo electrónico no solicitado causa a empresas e individuos. No existe fundamento para su aplicación, pero su eficiencia, como en la mayoría de los temas de tecnología, favorece su utilización⁷.

C. Legales: acciones judiciales y legislación

Acciones judiciales

Teniendo en cuenta que buena parte del contenido que se difunde mediante envíos masivos indiscriminados es fraudulento, las leyes penales tradicionales son un instrumento adecuado para reprimir esas conductas. Lo electrónico dificulta en algunas ocasiones la recolección y presentación del material probatorio.

El acceso ilegal o abusivo a los sistemas de información es un tipo de conducta penal de reciente aparición en varias codificaciones, que pretende englobar las conductas contrarias a la intimidad de los individuos. En el caso de las empresas, la intimidad no se protege sino que se penalizan los actos contra competidores comerciales mediante la desorganización interna de los competidores ha sido otra forma de penalización general de actos contra competidores comerciales.

7 ALAN SCHWARTZ y SIMSON GARFINKEL. "Stopping Spam – Stamping out unwanted e-mail news posting", O'Reilly Media, 1998.

La utilización de direcciones de dominio ficticias, el engaño técnico de suplantación de los encabezamientos de mensajes electrónicos y la utilización de la reputación de marcas o derechos de autor para falsear veracidad de los contenidos de un correo electrónico son actividades ilícitas que han surgido directamente del *spamming*.

Tales conductas han sido reprimidas legalmente al establecer protección específica al consumidor, aplicación analógica de figuras y categorías tradicionales, o mediante la creación de obligaciones nuevas propias del entorno digital, como el marcado o etiquetado de los mensajes con el fin de determinar su clasificación. En Colombia, por ejemplo, el primer caso relacionado con correo electrónico no solicitado tenía como supuesto fundamental la no remoción de la lista de direcciones de correo del emisor a pesar de su supuesta insistencia⁸.

La utilización de la infraestructura de los PSI, para enviar correos masivamente, ha originado que éstas cada vez con mayor frecuencia incluyan cláusulas contractuales en las cuales se prohíban tales conductas y se permita la terminación anticipada del contrato. El ejercicio de tal facultad ha originado pleitos entre los PSI y sus contratantes.

Legislación

Los dos principales modelos de regulación son el estadounidense y el europeo. Históricamente en los Estados Unidos fue donde primero se presentaron problemas asociados con el correo masivo no solicitado.

También en Estados Unidos se entablaron los primeros casos judiciales de manera masiva contra individuos que se presumía utilizaban la red global para enviar mensajes comerciales no solicitados⁹. Con el paulatino desarrollo del comercio electrónico en la Unión Europea, la regulación a

8 [www.alfa-redi.org/upload/revista/80403--0-7-diaz082003.pdf].

9 [www.news.com.com/2100-1028_3-5128806.html?tag=st_lh].

través de directivas con referencia específica al tema ha adquirido mayor importancia.

III. EL MODELO ESTADOUNIDENSE

Tanto a escala federal como estatal se ha intentado combatir el *spamming* con la legislación específicamente diseñada para tal efecto. Las razones principales de esta legislación han sido la defensa de los intereses de los consumidores y evitar actividades fraudulentas en línea.

Veinticuatro estados han establecido leyes especiales contra el *spamming*: Arkansas, California, Colorado, Connecticut, Delaware, Idaho, Illinois, Iowa, Kansas, Louisiana, Maryland, Minnesota, Missouri, Nevada, North Carolina, Ohio, Oklahoma, Rhode Island, South Dakota, Tennessee, Utah, Virginia, Washington y West Virginia. Varios intentos a escala de legislación federal fueron hechos hasta la entrada en vigencia de la ley federal CAN-SPAM Act/2003.

Respecto de esta ley federal se presentaron más de 12 proyectos al Congreso de los Estados Unidos con diferentes modelos de regulación, desde el *opt-out* hasta el proteccionismo absoluto a los PSI. Finalmente, en diciembre de 2003 se aprobó el CAN-SPAM Act (Controlling the Assault of Non Solicited Pornography and Marketing Act). Esta ley permite a la Comisión Federal de Comercio y a los proveedores de servicios de internet demandar a los individuos y compañías que utilicen falsos encabezamientos en sus correos electrónicos, que no permitan a los suscriptores ser excluidos de los listados de correo o que envíen un volumen de mensajes a direcciones obtenidas sin el consentimiento de los receptores.

Las sanciones en esta regulación incluyen el pago de los perjuicios causados por el correo electrónico no solicitado, así como multas (*statutory dammages*) de hasta 6 millones de dólares y la posibilidad de prisión de hasta 5 años en los casos más graves.

El CAN-SPAM Act impone diversas obligaciones al emisor de mensajes de datos, entre las cuales se deben destacar las

siguientes: no se puede utilizar información falsa que evite la identificación de quien realmente envía el mensaje, se debe identificar al correo como publicitario, debe especificarse la posibilidad de ser excluido de la lista de correo y esta solicitud del consumidor debe ser atendida en un período de máximo 10 días hábiles desde la solicitud, el mecanismo de exclusión debe ser mantenido al menos durante 30 días desde el mensaje original, no se puede utilizar la dirección de correo electrónico de un tercero para enviar mensajes.

El CAN-SPAM Act ha sido criticado desde varios frentes: en los primeros meses de su aplicación el número y volumen de correos electrónicos no solicitados aumentó, lo que ha puesto en duda su eficacia y por el hecho de coincidir con la puesta en marcha de una legislación estatal en California, más estricta, a la cual la ley federal se sobrepone en sus efectos.

La ley antispam de California debió haber entrado en vigor en enero de 2004, a menos que se considere, como efectivamente se está discutiendo, que esa ley federal atrás reseñada prima en su aplicación. La ley de California adopta un esquema *opt-in*, es decir, en el cual se definen en la ley las características del *spamming* así como las sanciones, y éstas pueden ser aplicadas salvo el consentimiento expreso del consumidor. En el esquema *opt-out*, por el contrario, la razón de ser de la regulación es permitir al usuario ser excluido de la lista de correos a posteriori y por lo tanto con efectos hacia el futuro. Esta ley prohíbe el envío de correo electrónico de contenido comercial (a) por cualquier persona localizada en California o (b) a una dirección de correo electrónico localizada en California a menos que el receptor haya expresado el consentimiento de recibir el mensaje o si existe una relación personal o comercial previa entre el emisor y el receptor del mensaje.

La ley también prohíbe la recolección, el uso o el registro de diversas direcciones de correo electrónico con el propósito de enviar *spamming*. El envío de mensajes de datos en que se suplante el nombre del emisor o con contenido que lleve a error al receptor sobre el mensaje también es reprimido.

A diferencia del CAN-SPAM Act, la ley establece una acción en cabeza de los individuos afectados, y legitima al procurador general y a los proveedores de correo electrónico para tal fin.

Las sanciones establecidas en la ley californiana se tasan en \$1.000 USD por cada mensaje infractor hasta un máximo de \$1.000.000 USD por incidente de *spamming*.

La redacción amplia de la ley de California la hace vulnerable a posibles ataques por inconstitucionalidad, al violar el derecho de libre expresión e interferir en la libertad de comercio de otros estados.

Las legislaciones estatales de los Estados Unidos de América pueden clasificarse en:

A. Antifraude

Con este tipo de legislación se ha tratado de evitar que el correo electrónico contenga información falsa en cuanto a la identidad del emisor o los recursos técnicos utilizados para el envío, por ejemplo, la dirección de correo electrónico y el contenido propiamente dicho.

Para cumplir con ese tipo de regulaciones, simplemente se debe proceder con buena fe en el uso de las direcciones de correo electrónico que posee el individuo a la empresa. Una empresa de mercadeo, por ejemplo, que cumpla los estándares de ética de ese oficio, cumpliría plenamente estas regulaciones.

Las legislaciones estatales no son uniformes en cuanto a la legitimación para actuar por activa. La mayoría de los estados permite actuar como demandante al receptor de los mensajes, al proveedor de servicios de internet afectado y a cualquier otra parte que demuestre el perjuicio. Algunos estados autorizan expresamente las acciones de clase.

La mayoría de estas regulaciones contemplan sanciones penales, así como la posibilidad de reclamar perjuicios por la vía civil de hasta \$25.000 USD por la recepción de ese tipo de mensajes.

Entre las diversas formas de tasación de perjuicios se encuentran las siguientes: en Colorado tanto el receptor del mensaje como el PSI afectado pueden demandar por los perjuicios causados, más una pena adicional de 10 dólares como daño punitivo por cada mensaje recibido del emisor de los mensajes masivos. En Nevada, tal posibilidad es alternativa. En Tennessee, las posibilidades son 10 dólares por mensaje o 5.000 dólares por día de infracción a la ley. En Kansas, cada violación puede ser tasada entre 500 y 10.000 dólares. En Illinois, Carolina del Norte, Oklahoma y Utah, las sumas previstas son \$10 USD por mensaje enviado o 25.000 dólares por día.

El caso de Ohio es particular en atención a los montos previstos: 50 dólares por cada violación (hasta 50.000 dólares en total) más una suma adicional de 500.000 dólares si la violación fue internacional, y una suma ilimitada, dependiendo de las pruebas respectivas, si la violación implicó la suplantación de la dirección de origen del correo electrónico no solicitado. En Delaware, en la legislación más estricta, está prevista la figura del daño punitivo o ejemplarizante del triple del perjuicio compensatorio.

Desde la óptica penal, Arkansas, California, Connecticut, Delaware, Louisiana, Missouri, Carolina del Norte, Rhode Island, Dakota del Sur y Virginia han establecido penas de prisión y multas o cauciones por la violación de las leyes *antispamming*.

B. *Opt-out* (posibilidad de exclusión)

Otro tipo de regulación prevé la obligación de establecer mecanismos por parte de los emisores de mensajes para que los receptores puedan tener la opción en el futuro de no recibir mensajes de datos si ésta es su voluntad. La mayoría de las regulaciones que tienen como fundamento esquemas de *opt-out* obligan a que en el mensaje de datos enviado se incluya un número telefónico gratuito o una dirección de correo electrónico que permita expresar la voluntad del receptor. Bajo

estas regulaciones, en caso de recibir un mensaje en el que se exprese el *opt-out*, el emisor queda obligado a no enviar posteriores mensajes. El incumplimiento de estas reglas trae consigo sanciones civiles y penales.

C. Conformidad con reglas establecidas por los PSI

Puesto que los PSI son los principalmente afectados por el volumen de tráfico ocasionado por el *spamming*, la legislación de los estados otorga respaldo a las fórmulas contractuales por la violación de términos y condiciones de uso establecidas por los PSI en relación con el *spamming*. De esta forma se otorga respaldo legislativo a las fórmulas contractuales.

D. Aplicación extraterritorial (multijurisdicción)

El envío de mensajes de datos no solicitados trae consigo problemas respecto a la jurisdicción aplicable, que son evidentes en Estados Unidos como consecuencia del hecho de que emitir publicidad por medios electrónicos en el mercado interno implica publicidad interestatal. En las leyes *antispamming* de Ohio y Delaware se opta por la teoría de los efectos en esos estados, en el sentido de considerar que el acto de *spamming* puede ser tipificado bajo esas leyes estatales si los efectos se producen respecto a tales jurisdicciones.

IV. EL MODELO DE LA UNIÓN EUROPEA¹⁰

La regulación legal del *spamming* en la Unión Europea se ha llevado a cabo en etapas, las cuales han coincidido con las Directivas relacionadas con la protección de la intimidad de los individuos. La intimidad de los usuarios de internet ha

10 SERGE GAUTHRONET y ETIENNE DROUARD. "Unsolicited commercial communications and data protection", Commission of the European Communities, 2001.

sido la preocupación principal en la Unión Europea, como proyección de la corriente garantista de los datos personales y la intimidad que se inició en la década de los 1980.

A. Directiva 95/46/EC de 24 de octubre de 1995

Esta directiva general sobre protección de datos personales permitió la protección de las direcciones de correo electrónico, como datos personales de quienes las poseen, más aún cuando existe una relación entre la dirección y el nombre o apellido de un individuo.

De acuerdo con esta directiva, ningún dato personal puede ser procesado válidamente a menos que haya sido recolectado y tratado de buena fe y con unos propósitos legítimos. Para determinar la legitimidad del uso del dato se establece en la Directiva la constatación de un consentimiento libre y espontáneo, así como el uso adecuado de la información para propósitos que no contraríen los derechos fundamentales de los individuos.

B. Directiva 97/66/EC del 15 de diciembre de 1997

Esta Directiva incluye la regulación de dos estrategias de mercadeo directo, por lo que tiene una influencia fundamental en la lucha contra el correo electrónico no solicitado. Respecto de cualquier dispositivo automático para el envío de mensajes y telemercadeo, la Directiva exige el previo consentimiento del receptor.

El efecto de la Directiva en el régimen europeo contra el correo no solicitado es evidente, en la medida que, por ejemplo, algunos países miembros de la Unión, como Austria, Dinamarca, Finlandia e Italia, han incluido al momento de incorporarla a su régimen jurídico interno, el correo directo, en los fenómenos regulados por la Directiva.

C. Directiva 2000/31/EC en comercio electrónico del 8 de junio de 2000

Esta Directiva establece la obligación, para los Estados miembros que permitan el correo no solicitado, de garantizar que las comunicaciones sean identificadas de manera clara, plena y unívoca. También se deben adoptar medidas para que los proveedores de ese tipo de servicios respeten las listas de opción de exclusión (*opt-out*) recolectadas por entidades privadas.

Esta Directiva generó una gran discusión por su redacción en cuanto al modelo de represión contra el correo electrónico no deseado, que fue visto por algunos como favorable a los sujetos activos de esta conducta, en particular por la posibilidad de desactualización de las listas de usuarios, quienes quedarían desprotegidos, y por la posibilidad de que los emisores de mensajes masivos los demandaran.

D. Directiva sobre intimidad en las comunicaciones electrónicas (02/58/EC) de 2002

Esta Directiva hace parte del conjunto de regulación puesta en funcionamiento por la Unión Europea para fomentar el comercio electrónico, el uso de tecnologías de la información, y actualizar la protección urgente a la intimidad de los ciudadanos de la Unión Europea.

La Directiva prohíbe la práctica de enviar correo electrónico no solicitado sin el consentimiento previo del receptor, salvo en el evento en el que la dirección de correo electrónico de los usuarios/consumidores haya sido obtenida en el contexto de la venta de un producto o servicio. En este último caso se debe otorgar la posibilidad de que el consumidor o receptor de los mensajes pueda expresar su intención de ser retirado de la lista.

CONCLUSIÓN: CARACTERÍSTICAS DE LA CONVERGENCIA DE MODELOS DE REGULACIÓN DE *SPAMMING*

A manera de conclusión, y luego de esta descripción breve de los problemas fundamentales de la regulación del *spamming*, así como de los principales modelos regulatorios de este fenómeno de reciente aparición, se puede afirmar lo siguiente:

1.º La globalización del internet y demás tecnologías de la información ha impulsado la reflexión sobre modelos de regulación universal y unificada que permita disminuir los costos de transacción de los negocios electrónicos y reprimir las conductas contrarias al desarrollo de la red global o a la libre acción de los sujetos participantes.

2.º El *spamming* está en medio de dos tendencias extremas: el aprovechamiento de las posibilidades directas de publicidad de productos y servicios, por una parte, y el abuso de las características de la red global para amenazar la intimidad de consumidores y ciudadanos tanto como el tráfico normal en la red global, por la otra.

El dilema, en consecuencia, comienza por la determinación de las características que diferencian el envío de correo electrónico con propósito comercial o publicitario, del *spamming* propiamente dicho.

3.º El volumen de los mensajes y la forma de captación de las direcciones de correo electrónico de la parte de los emisores y el consentimiento o la ausencia del mismo desde la óptica del consumidor-receptor del mensaje son las variables más usuales para tipificar el *spamming*.

Los diferentes modelos de regulación dependen entonces de un análisis del fenómeno, con el fin de clarificar sus características en relación con el uso normal del correo electrónico como medio de comunicación.

4.º Desde la óptica del regulador, la definición de determinada característica del *spamming* tiene como consecuencia implícita o expresa, según el caso, la defensa de la publicidad en línea o de los derechos del consumidor, en particular el de intimidad.

5.º Cifras recientes demuestran que cerca del 53% de todo el correo electrónico que llega a los quince países de la Unión Europea son correo no solicitado. Se considera que el 80% del mismo proviene de los Estados Unidos¹¹.

6.º No existe unanimidad a escala internacional sobre cuál es la óptica, entre las dos citadas, que debe primar. En el contexto global tanto la defensa de la publicidad como del consumidor son el fundamento de las leyes contra el *spamming*. Tal divergencia puede ocasionar retraso en una solución realmente internacional a este problema.

7.º Es posible afirmar que existe una unidad de criterio, por lo menos en los bloques económicos más relevantes, respecto de la necesidad de combatir el *spamming* –o por lo menos su faceta negativa y cuestionable– por las graves consecuencias colectivas e individuales que éste causa. Algunos elementos convergen a tal fin, en particular la necesidad de definir el concepto de *spamming* y diferenciarlo de las categorías de mercadeo y publicidad legítimos.

8.º En Colombia cualquier regulación directa o indirecta del *spamming* deberá sopesar la necesidad de lograr una regulación que se integre al régimen global que se está construyendo, pues ésa es la única vía posible para reprimir un fenómeno con alcance internacional como éste. Deben tenerse en cuenta las experiencias extranjeras en cuanto a la correcta y completa definición del *spamming*, con el fin de evitar su confusión con la publicidad directa. Se deberá determinar si el régimen sancionatorio es civil y/o penal, así como las autoridades administrativas y/o judiciales que lo aplicarán. Desde la perspectiva del usuario, se deberá garantizar que éste sea protegido de antemano frente al correo masivo y no solamente cuando a posteriori haya expresado su intención de ser excluido de la lista del emisor.

11 En "US orders legislation on spam, cookies", en [www.usatoday.com/tech/news/internetprivacy/2004-04-01-eu-outlawsspam_x.htm].