REGULACIÓN DEL SPAM EN MÉXICO

Julio Téllez Valdés (*)

(*) Doctor en Derecho Informático (Universidad de Montpellier, Francia). Profesor investigador del Tec de Monterrey , campus estado de México, jatellez@itesm.mx

1) ORIGEN

Spiced Ham. En 1937 la empresa Hormel Foods lanzó un alimento enlatado que originalmente recibió el nombre de Hornel's Spiced Ham. El éxito que la carne en lata tuvo fue tal que la compañía decidió reducirle el nombre a cuatro letras: SPAM[1].

2) CONCEPTOS BÁSICOS

a) SPAM . Según definiciones de la NACPEC, el Spam es "el correo comercial no solicitado generalmente enviado a las direcciones electrónicas de los consumidores sin la autorización y consentimiento del consumidor, comúnmente es enviado por empresas de mercadeo o telemercadeo, compañías legítimas o por individuos comisionados exclusivamente para dicho fin"[2].

b) SCAM . Similar al spam, encontramos el término "*Junk mail*" o *Scam*[3] (correo chatarra) que es utilizado para referirse a correos relacionados con publicidad engañosa (enriquecimiento al instante, pornografía, premios, etc.) y cadenas[4] (correos que incluyen textos en donde solicitan ser reenviados a otras personas con la promesa de cumplir deseos, traer buena suerte o ganar dinero).

c) SPIM . Además del *Spam*, ha surgido una nueva vertiente de este tipo de ataque cibernético, denominado "*Spim"*, que es un tipo de *Spam* pero que en vez de atacar a través de los correos electrónicos, lo hace a través de la mensajería instantánea.[5]

d) PHISHING. Es una nueva modalidad de fraude en Internet contenida en sitios que se asemejan a los de los bancos, sistemas de pago o proveedores conocidos en los que generalmente se señala una falla en el sistema o que la información no ha sido debidamente actualizada y por lo tanto solicitan al

---

[1] Se dice que el término "Spam" se derivó de un capítulo de la famosa serie inglesa de los ochentas de nombre "Monty Pithon" en la que uno de los actores decía: "Well, we have Spam, tomato & Spam, egg & Spam, Egg, bacon & Spam…" A raíz de esto se comenzó a utilizar este término con la llegada del Internet. Actualmente Spam es una marca registrada de carnes que comúnmente vienen enlatadas . Este embutido alimentó a soldados soviéticos y británicos durante la segunda Guerra Mundial y en 1957 se comenzó a comercializar. En los años 60 se hizo más popular porque se le añadió una anilla de apertura automática.

[2] NACPEC . Preguntas más frecuentes acerca del Spam y Phising, http://www.nacpec.org/es/faq.html

[3] Impulsa Profeco campaña contra fraude cibernético. Notimex. El Universal, 21 de febrero del 2005. http://www.eluniversal.com.mx/pls/impreso/version_imprimir_supl?id_articulo=19203&tabla=articulos

[4] SPAMMING. http://www.enewnesslaw.com/spammingC.htm

[5] Coburn, Claudia. Lo que faltaba: Spim. http://www.netmedia.info/informationweek/articulos.php?id_sec=6&id_art=4665

consumidor acceder a una pagina Web por medio de un link, y que al ser abierto, los defraudadores solicitan información comúnmente de carácter personal: datos personales, números de cuenta de tarjeta de crédito o débito del cliente, passwords o NIP (número de identificación

e) SPAMMERS. Son personas o empresas que envían mensajes Spam y lo realizan con diferentes técnicas para conseguir listas muy grandes de correos que son necesarias para realizar su actividad.

La mayoría de los Spammers trabajan a través de programas automáticos, los cuales recorren la red buscando en sitios, foros, blogs, bases de datos, grupos de noticias entre otros.

Cuando adquieren la información de los correos electrónicos se encargan de enviar los mensajes a los destinatarios, esto se utiliza, la mayoría de las veces con fines comerciales, pero también puede ser con la intención de causar un daño con algún virus o incurrir en fraudes a través del Phising.

3) PROBLEMÁTICA

Internet ciertamente ha permitido rebasar fronteras y tener al alcance muchos tipos de información, sin embargo uno de los medios más utilizados como lo es el e-mail, frecuentemente es aprovechado por personas o empresas mal intencionadas que hacen envíos de correo masivos a personas que no lo han solicitado. El spam ocasiona congestionamientos en los servidores de correo ocasionando una disminución en el espacio disponible para sus usuarios, causando una perdida en el nivel de calidad del servicio. Cabe mencionar que este tipo de comunicaciones no deseadas pueden ser transmitidos por distintas vías, no solamente por correo electrónico, sino también en mensajes de texto vía teléfonos celulares y programas de mensajería instantánea, como el Messenger.

Como nos dice Cristos Velasco[6], este correo comercial no solicitado o chatarra, actualmente es uno de los grandes problemas que afectan a los consumidores que navegan en Internet puesto que su utilización y difusión por parte de las empresas e individuos representa un problema significativo de costo y pérdida de tiempo y recursos para las personas que utilizan el correo electrónico. Generalmente, el spam es enviado por empresas de mercadotecnia o simplemente por individuos contratados específicamente por empresas ilegítimas que se especializan en elaborar listas de distribución de correos electrónicos para enviarlos directamente a las carpetas de los usuarios y dichos mensajes comúnmente se filtran cuando el usuario no cuenta con las herramientas necesarias para identificar, controlar y eliminar el spam. Aún y cuando el usuario cuenta con las herramientas para controlar el spam, muchas veces los mensajes normalmente se filtran a las carpetas

[6] VELASCO, Cristos, *Protección al consumidor en el contexto de la sociedad de la información*, Revista Nova Iuris, ITESM-CEM, México, enero 2005, pag. 144. Dicho autor recomienda revisar la página GetNet Wise que contiene algunos tips y herramientas para controlar el spam, así como otros links con la Comisión Federal de Comercio de lo Estados Unidos para reportar el spam enviado a los consumidores. http://spam.getnetwise.org/

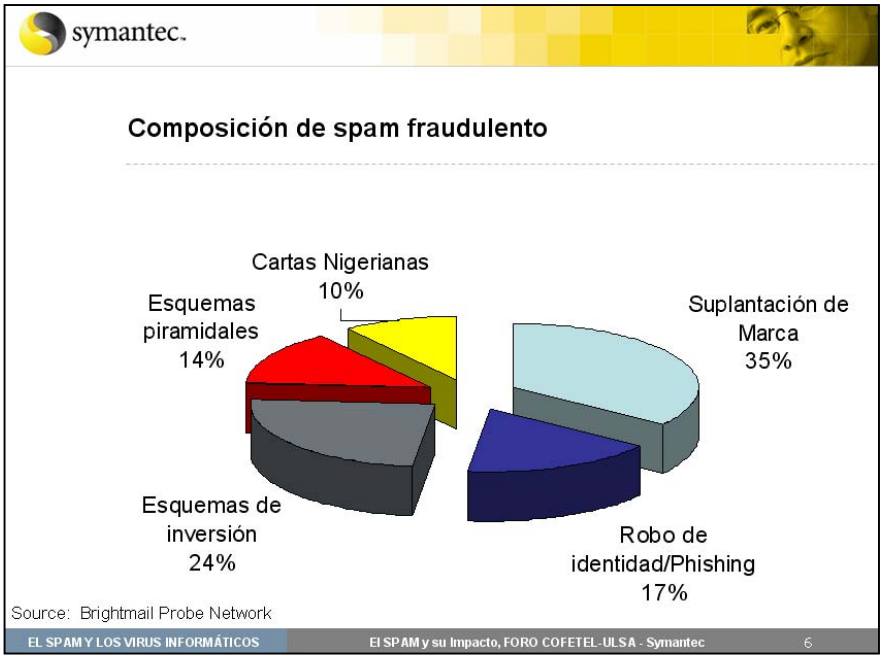
conocidas como “bulkmail”. Es a través del spam, que muchas empresas y proveedores de bienes y servicios llevan a cabo prácticas comerciales engañosas y fraudulentas hacia los consumidores y sobre todo ahora se ha convertido en un conducto para cometer otros ilícitos tales como el robo de identidad.

TIPO DE SPAM	DESCRIPCIÓN
Productos	Son los e- mail que ofrecen o aconsejan usar un determinado producto. Ejemplos: Servicios de investigación, maquillajes, prendas de vestir...
Financieros	Son los e- mail que contienen ofertas relacionadas con dinero. Ejemplos: Inversiones, préstamos, inmuebles...
Adultos	Son los emails que contienen o se refieren a productos o servicios dirigidos a personas mayores de edad (+18 años); suelen ser contenidos ofensivos o inapropiados. Ejemplos: Porno, anuncios personales, consejos matrimoniales...
Salud	Son los e- mails que ofrecen o aconsejan productos y/o servicios relacionados con la salud. Ejemplos: Farmacéuticos, tratamientos médicos, remedios con hierbas medicinales...
Engaños	Son los reconocidos como fraudulentos, intencionadamente equivocados, o conocidos para una actividad ilegal por parte del emisor. Ejemplos: Cartas nigerianas, esquemas piramidales, cartas en cadena...
Internet	Son los que específicamente ofrecen o aconsejan servicios o productos de o para Internet. Ejemplos: Servicios de hosting, diseño web, programas de filtrado de spam...
Ocio	Son los que ofrecen premios, descuentos en actividades de ocio, etc. Ejemplos: Ofertas de vacaciones, casinos on-line, juegos...
Fraudes	Son los emails que aparentan ser de compañías bien conocidas, pero no lo son. Esto es conocido como "Phising". Estos mensajes suelen usar trucos para revelar información personal de los usuarios, como la dirección de e-mail, información financiera, contraseñas, etc. Ejemplos: Verificación de tarjetas de crédito, notificación de cuentas, actualizaciones de facturación.
Políticos	Son los mensajes que aconsejan una campaña de un candidato político, piden que dones dinero a un partido o a una causa política, ofrecen productos relacionados con la campaña o figura del partido. Ejemplos: Partidos políticos, elecciones, donaciones...
Religión	Son los e-mails con información o servicios religiosos o evangelización espiritual. Ejemplos: Psíquicos, Astrología, religión organizada...
Otros	Son los e-mails que no pertenecen a ninguna de las anteriores categorías

El spam representa pérdidas millonarias para las empresas y gobiernos puesto que satura el tráfico de las redes corporativas y gubernamentales, invade las direcciones de correo del personal y muchas veces los mensajes al ser abiertos contienen virus que corrompen la seguridad de los equipos informáticos y de cómputo y por ende la productividad de los empleados.

Recientemente, el director para América Latina de Iron Port, Jorge Padres, en entrevista a la agencia noticiosa mexicana Notimex advirtió que las amenazas cibernéticas han presentado una evolución peligrosa, saliendo a la luz nuevas formas de atacar y cometer fraudes en la red surgiendo una nueva forma de obtener cuentas de correo para el envío de spam conocida como DHA (Directory Harvest Attacks). Explicó que el DHA son ataques que hacen los spamers para tratar de identificar cuentas de correo electrónico, que a diferencia de lo que antes se hacia con las cadenas en las que se veían las direcciones de otras personas, ahora se hace con un programa de cómputo.

Señaló que al ingresar una dirección inventada o predeterminada de correo electrónico ésta es verificada por la máquina, haciendo una serie de combinaciones con algoritmos hasta que acierta con un usuario existente y al cual se le puede mandar un spam[7]. El problema más importante que hay con el correo electrónico es que la gente usurpa las identidades, pues manda un correo que podría corresponder a alguien conocido, pero sin que exista algo que asegure que es real



[7] *Entrevista a NOTIMEX , junio 2005. Este directivo afirmó que ahora se puede forzar y violar el protocolo de Internet tan fácilmente que cualquiera podría hacerlo. De igual forma dijo que se espera que 2005 sea un año muy importante en cuanto al ataque de correo basura y generación de virus, porque ahora son generados por computadoras "zombies" ya que desde 2004 las empresas dedicadas a generar correo basura pagaron a los creadores de virus para que desarrollaran un sistema zombie, que se refiere a un código que envía spam desde un servidor legítimo, lo que permite que pase los filtros que las protegen de estos ataques. Destacó que la situación se agrava porque las redes de zombies son utilizadas también para enviar correos electrónicos fraudulentos, como es el caso del phishing, mediante el cual obtienen información confidencial sobre cuentas bancarias o tarjetas de crédito.*

4) MEDIDAS PROPUESTAS POR ENTIDADES INTERNACIONALES

a) Unión Europea

De acuerdo con el artículo 5 de la Directiva 97/66/CE, los estados miembros deben prohibir cualquier forma de interceptar o vigilar comunicaciones por parte de cualquier persona que no sea su remitente o su destinatario salvo que esté legalmente autorizada. La aplicación y ejecución de la Directiva 97/66/CE estipula que se debe respetar los principios de la protección de datos personales, sobre todo a lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios.

b) Organización para la Cooperación del desarrollo económico (OCDE)

Los Lineamientos sobre Protección al Consumidor de la OCDE contemplan dos recomendaciones sobre el Spam en el principio general II relativo a la "Equidad en las Prácticas Empresariales Publicitarias y de Mercadotecnia" señalando que *"las empresas deben desarrollar e implementar procedimientos efectivos y fáciles de usar, que permitan a los consumidores manifestar su decisión de recibir o rehusar mensajes comerciales no solicitados por medio del correo electrónico; y cuando los consumidores manifiesten que no desean recibir mensajes comerciales por correo electrónico, tal decisión debe ser respetada*" [8].

Debido a la problemática que ha generado el spam a nivel mundial, la OCDE mediante el auspicio de la Comisión Europea organizó en Febrero del 2004 en Bruselas, Bélgica un taller de trabajo dedicado particularmente a analizar la problemática del Spam. Una de las propuestas más polémicas que se generó en el marco del taller de trabajo fue que la Unión Europea propuso la adopción de un Código de Conducta para combatir el spam, cuya propuesta no fue bien recibida por la Comisión de Comercio de los Estados Unidos ya que la mayoría del spam se genera en la Unión Americana[9].

En Septiembre del 2004, la OCDE llevó a cabo en Busan, Korea la segunda parte del taller de trabajo sobre Spam, esta vez auspiciado por el Ministerio de Información y Comunicaciones de Corea. El objetivo fue ahondar con mayor detalle acerca de la problemática que representa el spam Como resultado de este taller de trabajo, se comenzaron los trabajos de una iniciativa conocida como "Anti-Spam Tool Kit" para combatir el spam[10]

Finalmente en Agosto del 2004, la OCDE anunció la creación de un grupo Anti-Spam (Anti-Spam Task Force) que consiste en otra iniciativa que reúne a expertos (tanto del ámbito técnico como jurídico) en la materia provenientes de distintos sectores, (tales como gobierno, empresas, sociedad civil y

[8] VELASCO, Cristos, *Protección al consumidor en el contexto de la sociedad de la información*, Revista Nova Iuris, ITESM-CEM, México, enero 2005, pag. 145 y ss.
[9] Las memorias y documentos de este primer taller de trabajo de la OCDE sobre Spam se encuentran disponibles en: http://www.oecd.org/dataoecd/55/32/31450810.pdf
[10] Actualmente el "Anti-Spam Toolkit" se encuentra en proceso de elaboración, para mayores detalles ver la página de la OCDE disponible en: http://www.oecd.org/document/50/0,2340,en_2649_34267_33732274_1_1_1_1,00.html

academia) de los 30 países de la OCDE, incluyendo la Comisión Europea, con el objeto de establecer mecanismos de cooperación ágiles para combatir el spam y a los spamers a nivel mundial[11]. Para la OCDE , el problema del spam tiene mayores consecuencias económicas en los países llamados *emergentes* que en aquellos desarrollados.

c) Unión Internacional de Telecomunicaciones (UIT)

En Julio del 2004, la UIT organizó un taller de trabajo en Ginebra específicamente dedicado a analizar la problemática del spam con vistas a la creación de un marco de trabajo entre sus miembros para fomentar la cooperación internacional en materia de spam. Este taller de trabajo se originó con motivo de la instrumentación de la *"Declaración de Principios y el Plan de Acción"* adoptado el 12 de Diciembre del 2003 durante la primera fase de la Cumbre Mundial de la Sociedad de la Información y en preparación a la segunda fase que se realizará en Túnez en Noviembre de 2005.

Dentro de los resultados de este taller de trabajo sobre spam se dieron algunas recomendaciones tales como: (i) proporcionar ayuda y coordinación para países en desarrollo; (ii) la necesidad de abordar la problemática del spam en forma amplia mediante la participación del sector publico, privado, academia y sociedad civil, implementar soluciones técnicas; conscientizar y educar al consumidor, implementar legislación adecuada junto con mecanismos de ejecución viables e iniciativas de la industria; (iii) establecer mecanismos de cooperación entre otras organizaciones internacionales tales como la OCDE, ICPEN y la Internet Society; (iv) el establecimiento de legislación anti-spam entre países miembros de la UIT; (v) el establecimiento de un memorando de entendimiento que establezca soluciones globales para combatir el spam; y (vi) proporcionar a los miembros de la UIT una lista de contactos e información acerca del spam, así como información de la legislación anti-spam de cada administración para poder facilitar el dialogo y la cooperación en el futuro entre los países miembros[12].

---

[11] "OECD Task Force to Coordinate Fight Against Spam", disponible en el sitio de la OCDE en: http://www.oecd.org/document/7/0,2340,en_2649_22555297_33656711_1_1_1_1,00.html
De acuerdo al primer reporte de la OCDE sobre el spam en países emergentes, en promedio un ISP invierte en servicios de banda ancha utilizados por el spam 6 mil 300 dólares, más 5 mil 400 por su almacenamiento y 75 mil dólares en la administración por los abusos en el correo, sin contar con los costos de soporte para los usuarios finales.
Eso, sin contar los costos por licencias de filtros antispam, administradores para bloquear los ataques masivos y la protección contra riesgos adicionales como virus, programas espía (spyware), de control a distancia de la PC (bots) que vienen junto con el spam, puntualiza la OCDE.
"Al final, los ISP cargan en la factura de sus usuarios esos costos, que representan en promedio 10 por ciento del pago mensual por la conexión a internet", detalla.
Los 'spamers' desarrollan diversas tácticas para evitar ser detectados y toman sin permiso los recursos de otros usuarios para generar grandes cantidades de correo basura sin grandes inversiones.
La OCDE afirma que el impacto del correo basura en las economías en desarrollo es mayor por el bajo nivel de penetración de internet, el alto costo de la infraestructura y aplicaciones, así como la falta de personal calificado para su control y prevención.
"Eso ocurre en particular en el centro de Asia y naciones africanas, como Nepal y Nigeria, donde las conexiones no son mediante cables sino por conexiones vía satélite".
Otros factores que agudizan el problema del spam es que esas naciones no cuentan con una legislación apropiada para combatirlo ni acuerdos internacionales, y la protección para el usuario y su datos personales esta fragmentada.

[12] Las conclusiones del "ITU WSIS Thematic Meeting on Countering Spam" están disponibles en: http://www.itu.int/osg/spu/spam/

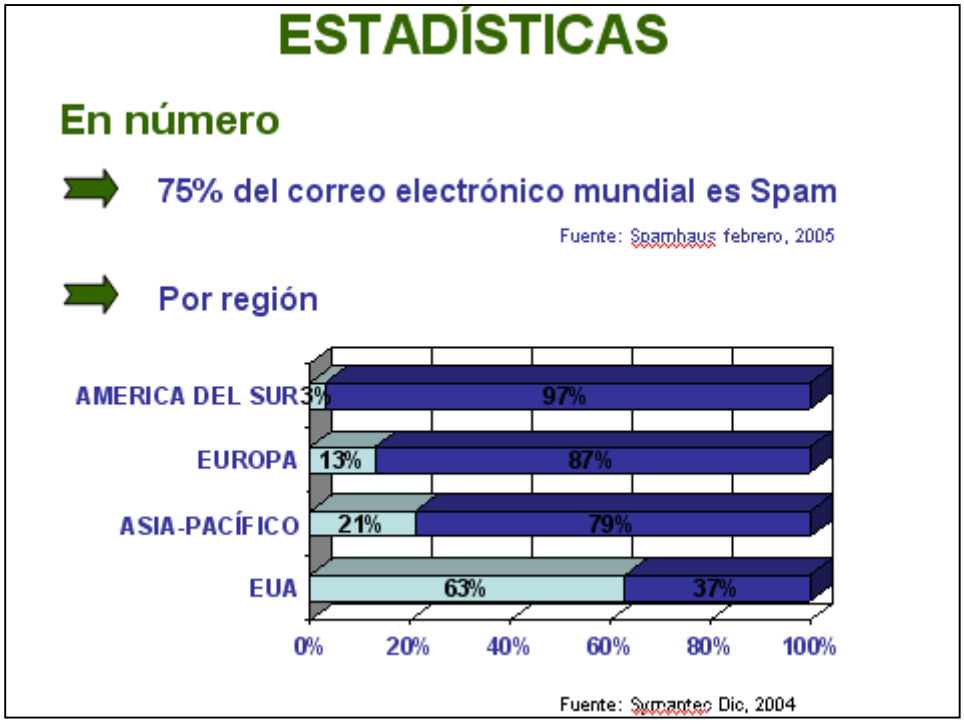
d) Otros

Asimismo, algunas agencias de protección al consumidor han celebrado acuerdos de entendimiento para combatir conjuntamente el spam y el phishing en sus territorios. Por ejemplo, en Julio del 2004, la Comisión Federal de Comercio de los Estados Unidos (US Federal Trade Commission), la Agencia del Comercio del Reino Unido (UK Office of Fair Trading) y la Comisión sobre Competencia y Consumidor de Australia (Australian Competition and Consumer Commission) celebraron un memorando de entendimiento para que las tres agencias puedan compartir información; cooperar en la investigación y detección de conductas anti-spam; rastrear y monitorear spammers y facilitar y coordinar su ejecución[13].

Por otro lado, las empresas más importantes que ofrecen servicios de correo electrónico como lo son Microsoft y Yahoo!, han incluido filtros en sus sistemas que ayudan a sus usuarios evitar que reciban este tipo de correos .

5) ALGUNOS DATOS A NIVEL MUNDIAL

Se dice que algunas cifras permiten considerar que tres cuartas partes (75 por ciento) del correo electrónico mundial es spam; de ese porcentaje, 63% se produce en Estados Unidos; 21% en la región Asia Pacífico; 13% en Europa, y 3% en América del Sur.



Por ejemplo, Hotmail reporta lo siguiente :
- el 83% de su correo es basura.

[13] "Consumer Protection Cops Join Forces to Fight Illegal Spam Six Agencies on Three Continents Will Leverage Law Enforcement Efforts", disponible en el sitio de la FTC en: http://www.ftc.gov/opa/2004/07/mou.htm

- en un día normal a través de ese administrador de correo pasan entre 2.4 y 3 mil millones de correos.
- en general, el correo rechazado por filtros antispam de los proveedores es de 80 por ciento.
- el Porcentaje de spam que llega a los usuarios es de 15%.

En lo que fue su primera acción formal contra la difusión de material ilegal a través de correo electrónico basura , el gobierno de Estados Unidos, a través de un juez federal de Las Vegas, Nevada, accedió el 5 de enero de 2005 a solicitud de la Comisión Federal de Comercio (FTC en inglés) a imponer restricciones a seis compañías y a sus directivos por presunta violación de las normativas que regulan el correo electrónico comercial. Las firmas afectadas fueron Global Net Solutions, Open Space Enterprises, Southlake Group y WTFRC, todas ellas con sede en Las Vegas, además de Global Net Ventures, de Londres, y Wedlake, con base en Riga (Letonia).

A estas empresas, y a algunos de sus directivos, se les acusa de enviar miles de correos sin incluir la advertencia obligatoria de "contenido sexual explícito", de prometer falsamente la adhesión gratuita a sus respectivas páginas web y de impedir que los destinatarios puedan dejar de recibir los correos indeseados.

Se presume, entonces, que violaron la ley contra este tipo de correos aprobada el 2003 por el Congreso de EE.UU, por lo que los acusados enfrentan una condena de prisión o a multas superiores a los 250 mil dólares, mientras que las empresas podrían pagar hasta medio millón de dólares .

Por otro lado Jeremy Jaynes (conocido bajo el seudónimo de *Gaven Stubberfield* y originario de Raleigh, Carolina del Norte), es la primera persona en ser condenada a prisión en Estados Unidos por envío de spam, en este caso nueve años de cárcel por un tribunal de Virginia . Jaynes era el spamer más prolífico del mundo y se embolsaba entre 500 mil y 750 mil dólares al mes gracias a estos spam, principalmente pornográficos.

La fiscalía presentó más de 53 mil pruebas de correos electrónicos ilegales enviados por Haynes, con nombre falso y falsa dirección de origen. Las autoridades también estimaron en 10 millones el número de mails enviados cotidianamente por Haynes a través de 16 líneas de alta velocidad, quien poseía ilegalmente una base de datos de los miembros de America on Line (AOL) los que representaban 84 millones de direcciones de correo electrónico.

Por otro lado, en España, la Agencia Española de Protección de Datos ha realizado cerca de 100 investigaciones sobre correos basura o spam , de las cuales se han resueltos 6, declarándose dos infracciones graves por ser comunicaciones comerciales masivas (con multa de 30,000 euros cada una) y dos leves. En dos casos se han archivado las actuaciones.

Cabe mencionar que en Argentina, un juez federal el 11 de noviembre pasado, impuso a un demandado de no enviar más correos spam con los datos de los demandantes, los abogados Gustavo Tanus y Pablo Palazzi, especialistas en Internet y protección de datos, en el primer fallo de tribunal que implica el

correo electrónico de "bulto" voluntario en Argentina (*Tanus v. Cosa en Datos Habeas,* Alimentados. Civ. y Com. Ct., el No 1791/03, el 11/11/03) y basado en la Ley 25326, sobre Protección de Datos Personales.

En julio del año pasado, un juez en Colombia, basada en los Datos Habeas (derecho a la intimidad de información) la cláusula de la Constitución, ordenó que una compañía dejara de enviar correos electrónicos voluntarios a un recipiente que litigó. El Juez colombiano Alexander Diaz Garcia del Segundo Tribunal de Municipalidad en Rovira, el Departamento de Tolima, pidió Tarjeta Virtual, un correo electrónico, multimedia, y firma de e-asesor-financiero, dejar de enviar correos no deseados a Juan Carlos Samper, que demandó después repetidamente y sin éxito tratando de optar de la lista de direcciones de la Tarjeta Virtual (Caso el No 73-624-40-89-002-2003-053-00.)

En Brasil, el senador Helio Costa en agosto presentó una Cuenta de Ley conforme a la cual las compañías serían permitidas enviar un mensaje de spam sólo una vez y serían requeridas revelar su materia e identificar el nombre y dirección del remitente en el cuerpo del correo electrónico.

La cuenta, ahora en la discusión en el nivel de comité, prohibiría firmas enviar de nuevo tales mensajes sin el consentimiento previo del recipiente. Esto también daría a recipientes el derecho de solicitar que Proveedores de Internet bloquearan mensajes entrantes no autorizados dentro de un período de 24 horas.

Al mismo tiempo, una serie de Sitios Web y grupos de antispam sin fines de lucro han comenzado a surgir y difundirse , tales como Rompecadenas (http://www.rompecadenas.com.ar/index.htm) en Argentina y Anti Spam (http://www.antispam.org.br) en Brasil, ofreciendo herramientas y utilidades de punta para impedir al correo electrónico masivo saturar las cuentas de los usuarios.

6) SITUACIÓN EN MÉXICO

a) Algunos datos a nivel nacional

México es considerado como uno de los países en los que se presenta un mayor número de correos Spam (basura), de acuerdo con los resultados del estudio denominado Sweep Day 2005 en el que participaron 26 países, realizado el 21 y 22 febrero de 2005 por la Red Internacional de Protección al Consumidor y de Aplicación de la Ley (ICPEN), colaborando 77 organismos públicos y privados de todo el mundo, destacando en México la UNAM, PROFECO, CONDUSEF, AMIPCI, Microsoft México y T1msn[14].

Según este estudio, las empresas extranjeras son las responsables del 80% del correo basura que se distribuye en México, de donde el 20% corresponde a organizaciones legalmente constituidas y el 10% ciento distribuye información

[14] Algunas de las categorías que este año fueron reportadas en las que se utiliza el Spam para promoción son software y equipo de cómputo, productos farmacéuticos para adultos, servicios financieros y productos para el cuidado del cuerpo. En el caso de México, es la primera vez que el sector privado participa en este ejercicio, en el cual colaboran instituciones que manifiestan una preocupación por los problemas de Spam entre otros temas relacionados, como el comercio electrónico.

falsa, engañosa y fraudulenta. De acuerdo a NIC México, el uso de la la red para el envío de correo basura (spam) representa para los proveedores de acceso a internet (ISP) en el país un costo de 6.5 millones de pesos al mes, y para los usuarios encarece en 10% el precio por estar conectado, cada día llegan a usuarios en México mil 460 millones de correos spam, cuyo peso en promedio es de 5 kilobytes, es decir, los proveedores transmiten casi 7 terabytes de esos mensajes.

Los principales correos basura de contenido engañoso (scam) que llegan a México son las ofertas de trabajo fácil en casa para ser millonario, productos milagrosos para bajar de peso, la carta nigeriana y la venta de títulos profesionales piratas. El primer tipo de fraude se presenta como una oferta de trabajo del esquema piramidal, donde los miembros van reclutando nuevos miembros a la empresa hasta volverse millonario, sin embargo, para conocer el plan de negocios las personas tienen que pagar entre 200 y 300 dólares y nunca reciben la información.

De esta forma, de los dos billones de correos electrónicos que fluyeron por Internet en 2004, alrededor de 75 por ciento fueron spam, que en países como México representa un peligro mayor al considerar que las compañías nacionales sólo destinan en promedio a la seguridad informática entre 3 y 4% de sus presupuestos de tecnologías de información .

b) Regulación jurídica

Desde finales de 2003, la Procuraduría federal de Protección al Consumidor (PROFECO) colaboró activamente con países miembros del comité de políticas del consumidor (CCP) para la elaboración de un documento titulado: *Background Paper on Spam* en donde se hace un análisis del problema del spam y trata de esbozar las herramientas legales que posee cada una de las agencias con la finalidad de combatir esta práctica electrónica.

Posteriormente, como resultado de las reformas a la LFPC del 4 de Febrero del 2004, la PROFECO reforzó y mejoró el marco jurídico en los siguientes rubros: (i) las prácticas de mercadotecnia y de publicidad con el objeto de proteger al consumidor mexicano de los mensajes no solicitados que constantemente envían empresas de telemercadeo y publicidad por correo electrónico; (ii) veracidad de la información sobre bienes y servicios para evitar prácticas abusivas o engañosas por parte de empresas y proveedores; (iii) celebración de contratos de adhesión por vía electrónica y servicios adicionales o conexos no previstos en el contrato original; (iv) la presentación de denuncias por vía electrónica por incumplimiento a las disposiciones de la LFPC, la Ley Federal de Metrología y Normalización, normas oficiales mexicanas y demás disposiciones aplicables; y (v) las notificaciones de PROFECO por vía electrónica u otro medio similar previa aceptación por escrito del consumidor.

Las reformas más importantes en materia de prácticas publicitarias y de mercadotecnia se presentaron en los artículos 17, 18 y 18 BIS de la Ley Federal de Protección al Consumidor, relativos a la publicidad que se envía a

los consumidores en forma electrónica y el registro público a cargo de la PROFECO sobre los consumidores que no desean recibir dicha información o publicidad por parte de las empresas.

ANEXOS

ANEXO 1 : LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR (ARTÍCULOS RELEVANTES)

Artículo 17.- En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría. El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial".

Artículo 18. ……

La Procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito".

Artículo 18 BIS.- Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el artículo anterior. Los proveedores que sean objeto de publicidad son corresponsables del manejo de la información de consumidores cuando dicha publicidad la envíen a través de terceros".

(ii) En cuanto a la veracidad de la información sobre bienes y servicios para evitar prácticas abusivas o engañosas por parte de las empresas, se reformó el artículo 32 de la LFPC el cual dispone lo siguiente:

Artículo 32.- La información o publicidad relativa a bienes, productos o servicios que se difundan por cualquier medio o forma, deberán ser veraces, comprobables y exentos de textos, diálogos, sonidos, imágenes, marcas, denominaciones de origen y otras descripciones que induzcan o puedan inducir a error o confusión por engañosas o abusivas.

Para los efectos de esta Ley, se entiende por información o publicidad engañosa o abusiva aquélla que refiere características o información relacionadas con algún bien, producto o servicio que pudiendo o no ser verdaderas, inducen a error o confusión por la forma inexacta, falsa, exagerada, parcial, artificiosa o tendenciosa en que se presenta.

La información o publicidad que compare productos o servicios, sean de una misma marca o de distinta, no podrá ser engañosa o abusiva en términos de lo dispuesto en el párrafo anterior. La Procuraduría podrá emitir lineamientos para la verificación de dicha información o publicidad a fin de evitar que se induzca a error o confusión al consumidor".

(iii) En cuanto a la celebración de contratos de adhesión por vía electrónica y servicios adicionales o conexos no previstos en el contrato original se reformó el artículo 86 BIS para quedar de la siguiente forma:

Artículo 86 BIS. En los contratos de adhesión de prestación de servicios deben incluirse por escrito o por vía electrónica los servicios adicionales, especiales, o conexos, que pueda solicitar el consumidor de forma opcional por conducto y medio del servicio básico.

El proveedor sólo podrá prestar un servicio adicional o conexo no previsto en el contrato original si cuenta con el consentimiento expreso del consumidor, ya sea por escrito o por vía electrónica".

(iv) Con respecto a la presentación de denuncias por vía electrónica por incumplimiento a las disposiciones de la LFPC, la Ley Federal de Metrología y Normalización, normas oficiales mexicanas y demás disposiciones aplicables, se reformó el último párrafo del artículo 97 que contempla lo siguiente:

Artículo 97 …….

La denuncia podrá presentarse por escrito, de manera verbal, vía telefónica, electrónica o por cualquier otro medio.

(v) Por cuanto a las notificaciones de PROFECO por vía electrónica u otro medio similar previa aceptación por escrito del consumidor se reformó el penúltimo y último párrafo del artículo 104 que señalan lo siguiente:

Artículo 104 …….

Tratándose de actos distintos a los señalados con anterioridad, las notificaciones podrán efectuarse por estrados, previo aviso al destinatario, quien podrá oponerse a este hecho, así como por correo con acuse de recibo o por mensajería; también podrán efectuarse por telegrama, fax, vía electrónica u otro medio similar previa aceptación por escrito del interesado.

La documentación que sea remitida por una unidad administrativa de la Procuraduría vía electrónica, fax o por cualquier otro medio idóneo a otra

unidad de la misma para efectos de su notificación, tendrá plena validez siempre que la unidad receptora hubiere confirmado la clave de identificación del servidor público que remite la documentación y que ésta se conserve íntegra, inalterada y accesible para su consulta".

Finalmente, los artículos **126, 127, 128 y 128 BIS y 133** de la LFPC modifican el criterio para la cuantificación de multas, estableciéndose que las mismas habrán de referirse en cantidades fijas, para lo cual la PROFECO actualizará cada año las multas contenidas en dichos artículos en concordancia con los índices inflacionarios que contiene el Índice Nacional de Precios al Consumidor (INPC) publicado por el Banco de México. Dichas multas van desde los $150.00 hasta los $2,520,000.00 estableciéndose un límite máximo de infracciones hasta por la cantidad de $5,040,000.00.

ANEXO 2. PROPUESTA DE *LEY FEDERAL QUE REGULA EL CORREO ELECTRÓNICO*, PRESENTADA POR EL DIPUTADO JORGE LEGORRETA ORDORICA, DEL GRUPO PARLAMENTARIO DEL PVEM (29 DE SEPTIEMBRE DE 2004)

Exposición de Motivos

Con el uso de la Internet en conjunto, y el llamado correo electrónico o *e-mail,* se han dado prácticas y avances en estos medios, como la transferencia de audio, video, datos, telefonía por Internet, etcétera. Sin embargo, también se han desarrollado gradualmente prácticas que están resultando nocivas para todos los usuarios de Internet, y particularmente a los correos electrónicos, sean personales, empresariales, comerciales, etcétera.

El llamado correo electrónico tipo *spam* se considera actualmente como uno de los mayores problemas de seguridad informática, dándose casos en que hasta una tercera parte de los correos electrónicos son *spam*.

El correo *spam* se define como el mensaje de correo electrónico **no** solicitado por el receptor, usualmente distribuido a una lista de direcciones, cuyo contenido generalmente es de publicidad de productos o servicios; también puede ser de tipo comercial, u otro propósito: político, religioso, de hostigamiento, pirámides, advertencias de virus falsos; puede denominarse "correo basura". Este tipo de correo se puede clasificar en el comercial, que tiene por propósito vender algo, y el informativo, que proporciona datos sobre algún evento u ofrecimiento que no implica una erogación económica para el receptor.

Actualmente, ésta práctica tiene auge, debido a la facilidad que brindan las redes electrónicas para hacer llegar publicidad en poco tiempo y bajo costo de dinero a una gran cantidad de potenciales clientes (o víctimas). Es difícil calcular la cantidad de *spam* que circula por la Internet, sólo podemos concluir que se trata de porcentajes muy altos y verdaderamente preocupantes,

además el *spam* presenta otra serie de efectos secundarios, que no son comentados en los medios.

Desde el punto de vista de un usuario de Internet, el recibir *spam* se convierte en una molestia, pues no se puede tener una cuenta de "e-mail" o correo electrónico, para mantener comunicación seria con otras personas, y peor aún, si el usuario es un menor de edad, esta expuesto a invitaciones a sitios no aptos para su edad en el menos peligroso de los casos.

Las características más sobresalientes de un correo tipo *spam* es que son mensajes informativos no solicitados, y generalmente anuncian un sitio web con contenido pornográfico de cualquier tipo, o explican una forma para ganar dinero ("hágase millonario con sólo hacer un *click,* o al abrir este correo"), o un listado de productos para su venta, o bien regalan viajes u otras promociones que se convierten en fraudes ("usted se ha hecho ganador a un viaje todo pagado, para reclamarlo haga *click* aquí"). Además este tipo de envíos se realizan de manera masiva, es decir, que se reparten a miles de personas distintas a la vez, e incluso se llegan a repetir periódicamente.

Otra de las características de este tipo de correos es que el campo *from:* o "de:", es decir, el que envía dicho correo, generalmente contiene cualquier nombre ficticio, que no existe o es falsa la dirección de respuesta o *reply*. De igual manera los títulos de los correos contienen mala gramática, errores de ortografía, o bien se exagera en los signos de puntuación, ortografía o exclamación, se detectan la mayoría por ser títulos con combinaciones de nombres, letras o números.

Dentro de este tipo de correos existen diversas clasificaciones, con la idea de diferenciarlos se encuentran:

-UCE (Un solicited Comercial Emaill) También llamado Junk email (Correo Basura), el cual es un correo electrónico no solicitado de tipo comercial, cuyo contenido es propaganda sobre algún producto o servicio.

-UBE (Unsolicited Bulk Email) El cual es un correo electrónico no solicitado, enviado de forma masiva, es decir, a miles o millones de cuentas de correo. Este puede ser de tipo comercial, pudiendo también ser UCE, sin embargo, el contenido puede tener entre otros, propósitos políticos, religiosos, de hostigamiento, etc.

-MMF "Make Fast Money" (Haga Dinero Rápido) Es un correo que generalmente se presenta en forma de cartas cadena, o sistemas piramidales, cuyo contenido dice algo como: "¡Tu puedes ganar mucho dinero!, sólo envía dinero a la primera persona de la lista, borra el nombre y pon el tuyo en su lugar, y da un "forward" o reenvío de éste mensaje a otras personas".

-Correos electrónicos "Hoax", que significa en inglés "engaño", son correos electrónicos no siempre con fines comerciales, contienen

información falsa, y generalmente con contenidos mórbidos y mucho menos amigables que el clásico correo electrónico tipo *spam*. Su principal finalidad es que al ser enviado "de vuelta y regrese"; tras recorrer un largo camino; sirve para obtener listas de direcciones de correos electrónicos, que permiten al remitente al obtenerlas, vender éstas direcciones y realizar prácticas de *spam*.

-Usurpación de identidades, son correos electrónicos que aparentemente son enviados por una persona u organización, pero en realidad no es así. El propósito de estos correos es enviar información sobre un producto o servicio, pero sin importar cual sea el contenido del mensaje, se están haciendo pasar por otra persona u organización, provocando molestia en las personas que lo reciben, los cuales reclaman a la supuesta persona que los envío, quien en realidad también es víctima. Este tipo de correos incluso pueden considerarse como un ataque a la reputación de las personas.

Cabe destacar, que con el envío de este tipo de correos, existen varios afectados, que son:

1. El usuario del correo electrónico que lo recibe: que pierde tiempo y dinero al descargar mensajes que no ha solicitado, asimismo es molestado permanentemente con publicidad de cosas que no le interesan, y finalmente puede llegar un determinado momento en que dentro de su cuenta reciba más *spam*, que correos deseados.

2. El servidor al que pertenece la empresa o la persona que administra la cuenta de correo electrónico: en primer lugar porque el *spam* causa saturación del servidor, como ejemplo: imaginemos el envío de un millón de correos *spam* en tandas de 8,000 a 10,000 mensajes. Además si desde ese lugar se envían correos *spam*, el servidor puede ingresar a listas negras que existen dentro de Internet, de este modo, los administradores de Internet que consulten esas listas, bloquearán el acceso de todos los correos provenientes de ese servidor.

3. Finalmente, todos **los usuarios de Internet** resultan afectados, el estar transitando más de 500 millones de correos *spam* diario en todo el mundo, genera costos millonarios para todos los usuarios, en función de tiempo de conexión. De igual manera el incremento en el tráfico basura en las redes, empeora la calidad de las comunicaciones, y esto a futuro, puede llevar a que muchos usuarios dejen de usarlas. Incluso se han empezado a descubrir nuevas formas de *spam*, aprovechando el sistema de mensajería de los teléfonos celulares y PDAs (Personal Digital Agenda o Agenda Personal Digital), práctica que ya se da en países más avanzados.

Las desventajas o daños que causa al usuario de Internet el correo *spam*, son:

a) Usa recursos de otras personas, al ser una forma de vender publicidad no deseada, que obliga al receptor a pagar por recibirla,

mucho más de lo que le cuesta al remitente enviarla. Para recibir un correo *spam*, el usuario paga por un servicio de Internet, así como por el uso de la línea telefónica para realizar su conexión; por otro lado, el tráfico de millones de correos ejecutados en una sola vez y casi sin costo para el remitente, congestiona el uso de procesadores de las computadoras que prestan los servicios de Internet, y que de continuar ésta práctica, los servicios de Internet tendrán que enfrentar inversiones que encarecerán en mucho el costo del servicio.

b) Pérdida de tiempo, ya que la mayoría de estos mensajes piden al receptor que envíe un mensaje para remover su nombre de la lista de *spam*; lo que significa hacer algo para salir de una lista de la que nunca se autorizó formar parte. A menos que el título del correo sea muy obvio e indique un correo *spam*, el usuario debe perder tiempo al abrir el correo y leer un poco, para darse cuenta que se trata de un correo de éste tipo, aunado al tiempo que le tomará darse de baja de la citada lista.

c) Roban recursos, la dirección donde proviene el *spam*, generalmente no es la misma para comprar los productos, ya que los envíos de *spam* se hacen violando sistemas "inocentes" de terceras personas. Para evitar costos y bloqueos los *spamers* (personas que se dedican a realizar este tipo de prácticas), usan una técnica de "pegar y correr", enviando su correo desde distintos sitios, ya que es relativamente fácil violar un sitio de Internet para usar su canal de salida con éste tipo de propósitos, y finalmente los sitios usados con éste fin, tienen todo tipo de problemas, al ser rechazados por gran parte de la Internet siendo fuente "inocente" de *spam*. La mayoría de veces los *spamers* buscan servidores de correo de otras personas, que estén pobremente configurados, permitiendo así, el envío de correos de usuarios anónimos externos a su red. Otra forma utilizada es penetrar a servidores privados e instalar los programas de envío automático de correos, los cuales son controlados de forma remota, táctica que finalmente resulta difícil de bloquear pues éstos están cambiando constantemente de ubicación.

d) Se engaña al cliente o usuario; el costo de publicitarse es tan bajo, que cualquier oferta justifica el esfuerzo, asentando problemas de abuso al consumidor con ofertas engañosas o falsas de productos o servicios, algunas veces ficticios, apuntando a la búsqueda de personas que, por no estar correctamente informadas por éste tipo de prácticas, caen en éstos trucos. Como regla general, los productos que se ofrecen por *spam*, son lo suficientemente malos, que no justifican una campaña publicitaria formal.

e) Los usuarios son dañados, cuando el espacio de almacenamiento de sus cuentas de correo quedan saturados, en cuestión de días, por todos los mensajes *spam* recibidos, de forma que cuando otra persona quiera enviar un correo serio o de importancia, este no podrá entrar a su buzón, y si no se libera pronto el espacio suficiente para almacenarlo, el correo se perderá.

f) Generalmente su contenido es ilegal, al jugar con la disparidad de los diferentes marcos legales de protección al consumidor que existen en los países, y la dificultad para ubicar quien los envía, convirtiéndose en una excelente vía para promocionar productos o servicios ilegales o rechazables como cadenas de dinero, acceso a pornografía, difusión de pornografía infantil, etc. Por otra parte, la práctica de recolección y tráfico de direcciones, se basa en el engaño a los clientes y en falsas promociones para conseguir direcciones de usuarios. Y finalmente, la existencia de un mercado de direcciones de correo electrónico para hacer *spam*, ha abaratado enormemente la posibilidad de diseminar virus de todo tipo.

¿Cómo se obtienen las direcciones de correo electrónico víctimas del Spam?

Fácilmente se obtienen aprovechando las redes de computadoras mediante programas llamados "Web Spiders" (Arañas de red), para recorrer rápidamente páginas publicadas en Internet y extraer las direcciones de correo publicadas.

Otra de las formas es capturar datos de correos que viajan por Internet, donde las direcciones del remitente y del destinatario viajan en forma de texto plano, en cada correo que circula por la red, el contenido del mensaje puede traer direcciones de correo de otras personas, como cuando se reenvía un correo de tipo cadenas.

Estas direcciones capturadas, se recopilan en bases de datos que se venden por unos cuantos dólares o se intercambian entre *spamers*, y como consecuencia constantemente aparecen nuevos.

Frente a este tipo de conductas relativamente recientes que nacen en una tecnología con bondades y beneficios, es necesario regular las actividades nocivas, tanto para la vía Internet, como para lo usuarios. En la mayoría de los países donde existe legislación de éste tema, únicamente se establece que los correos no solicitados, contengan una etiqueta de identificación.

Estamos ciertos de la imposibilidad de regular la red, debido a que no tiene una pertenencia y su extensión es extraterritorial; por ello pretendemos con la presente iniciativa regular los servicios de conexión a la red y las conductas en la transmisión de los mensajes de correo electrónico, sancionando todo tipo de conductas que signifiquen falsificación o alteración en la información que contengan, y todo tipo de engaño. Del mismo modo se sanciona la duplicidad y la usurpación de identidad; para ello se propone crear una Comisión de Regulación del correo electrónico tipo *spam* con facultades para llevar registros, rastreo e investigaciones de oficio o basadas en denuncias o quejas.

Se establecen delitos especiales que se sancionarán equiparables al título V del Código Penal Federal "Delitos en Materias de Vías de Comunicación y Correspondencia"

Por las razones expuestas, sometemos a la consideración de esta soberanía la siguiente:

Iniciativa de Ley Federal que Regula el Correo Electrónico

Disposiciones Generales

Artículo 1. La presente ley es de orden público, y tiene por objeto regular al correo electrónico tipo *spam*, por ser una actividad nociva dentro de la Internet.

Artículo 2. Corresponde al Estado la Rectoría en materia de Telecomunicaciones incluyendo los servicios de conexión y/o transmisión vía Internet, por consiguiente sus prácticas, dentro de las cuales se encuentra el uso y aprovechamiento del correo electrónico o "e-mail", a efecto de proteger la seguridad y la soberanía nacional, la seguridad, tranquilidad y confidencialidad de los usuarios de correo electrónico o *e-mail* dentro de los sistemas y equipos de informática del Estado y de los particulares.

Artículo 3. Para efectos de ésta ley se define:

I. Mensaje de correo electrónico: todo mensaje enviado a una dirección de correo electrónico.

II. Dirección de correo electrónico: es el destino de un mensaje, expresado en una cadena de caracteres alfanuméricos, o nombre de usuario, o receptor, seguido o no, del nombre o caracteres alfanuméricos de un prestador de servicio de correo electrónico registrado en Internet.

III. Receptor: Toda persona que teniendo una cuenta de correo electrónico en Internet recibe un mensaje de correo electrónico dentro de su cuenta.

IV. Remitente: Toda persona que teniendo acceso a una conexión de Internet, envía un mensaje de correo electrónico a un receptor.

V. Correo electrónico tipo *spam*:

a) Todo tipo de mensaje de correo electrónico, no solicitado por el receptor, distribuido a una lista masiva de direcciones de correo electrónico, cuyo contenido sea de:

- Publicidad de productos o servicios;
- Contenido político o religioso;

- Juegos o apuestas;
- Contenido pornográfico de todo tipo, o bien conocidos en la Internet como Correos electrónicos tipo "Hoax";

- Comercio sexual;
- Información falsa;

- Sistemas piramidales o cadenas;
- Todo tipo de comunicación tendiente al engaño o al lucro.

b) Todos los correos electrónicos, no importando cual sea el mensaje, enviados por cualquier persona que se haga pasar por otro remitente, considerándose una práctica de usurpación de identidad.

Artículo 4. No se considera correo electrónico tipo *spam*, aquél mensaje de correo electrónico cuyo contenido sea publicidad de productos o servicios, de carácter comercial, político, religioso, juegos, pornográfico, sistemas piramidales o cadenas, o cualquier contenido similar, que sea solicitado expresamente por el receptor hacia el remitente.

Sin embargo, el receptor podrá solicitar en cualquier momento al remitente el retirar su consentimiento dado para recibir éste tipo de correo electrónico. En caso de que el remitente, posterior a que el receptor retiró su consentimiento, siga haciendo el envío de éste tipo de correos electrónicos, serán considerados correos electrónicos tipo *spam*, y por lo tanto sujetos a la regulación de la presente ley.

Artículo 5. A falta de disposición expresa en la presente ley, en los Tratados Internacionales o en su Reglamento; se aplicarán de manera supletoria las disposiciones expresas y/o análogas que se contienen en:

I. La Ley de Vías Generales de Comunicación.
II. La Ley Federal de Telecomunicaciones.
III. El Código Penal Federal.
IV. El Código Federal de Procedimientos Penales.
V. La Ley Federal de Procedimiento Administrativo.

Artículo 6. Queda prohibido a toda persona acceder a una computadora protegida, sin autorización, con la intención de iniciar la transmisión o envío de múltiples mensaje de correo electrónico tipo *spam*, desde dicha computadora.

Artículo 7. Queda prohibido:

I. Usar una computadora protegida, para enviar o retransmitir múltiples mensajes de correo electrónico tipo *spam*, con la intención de engañar o mal informar al o los receptores.

II. Acceder por medio de cualquier servicio de acceso al público a Internet, para enviar mensajes que engañen o mal informen al o los receptores.

Artículo 8. Queda prohibido alterar materialmente la información en los títulos de correo electrónico de carácter comercial, e intencionalmente iniciar la transmisión de dichos mensajes.

Artículo 9. Queda prohibido usar información que materialmente falsifique la identidad de una persona para:

I. Registrar varias cuentas de correo electrónico,
II. Hacerse pasar por un prestador de algún servicio de Internet,

III. Juntar, crear y/o comercializar conjuntos, grupos o listas de correos electrónicos,

IV. Intencionalmente iniciar la transmisión de correo electrónico tipo *spam*, usando combinaciones de dichas cuentas o nombres de prestadores de servicios de Internet.

Artículo 10. Queda prohibido, hacerse representar falsamente por un legítimo prestador de cualquier servicio de Internet, e iniciar, a nombre de éste, la transmisión de correos electrónicos tipo *spam*.

Artículo 11. Queda prohibido que cualquier persona inicie la transmisión, a una computadora protegida, de correo electrónico tipo *spam*, que contenga, o esté acompañada, de un título de correo electrónico o información, que sea materialmente falsa o engañosa.

Artículo 12. Queda prohibido hacerse pasar por una persona plenamente identificada por el receptor, para enviarle correo electrónico tipo *spam*.

Artículo 13. Queda prohibido iniciar la transmisión, hacia una computadora protegida, de correo electrónico tipo *spam*, y/o asistir en la creación de dicho correo, o en la selección de direcciones de correo electrónico a las que serán enviadas.

Artículo 14. Queda prohibido obtener direcciones de correo electrónico, usando cualquier sistema automatizado o software, de cualquier conexión a Internet que se encuentre dentro del territorio nacional, con el propósito de enviar correos electrónicos tipo *spam*. De igual manera, queda prohibida la creación, venta o distribución de cualquier tipo de software o sistema automatizado que facilite o permita el envío de cualquier tipo de correo electrónico tipo *spam*.

Artículo 15. Queda prohibido hacer uso de cualquier medio o programa de computadora, donde el remitente, genere posibles direcciones de correo electrónico mediante combinaciones de nombres, letras o números, con el propósito de enviar correos electrónicos tipo *spam*.

Artículo 16. Queda prohibido la utilización de cualquier medio electrónico automatizado para registrar múltiples cuentas de correo electrónico, o cuentas de usuarios en línea, para transmitir a una computadora protegida, cualquier tipo de correo electrónico tipo *spam*.

Artículo 17. Queda prohibido todo correo electrónico tipo *spam* con contenido sexual que:

I. Anuncie explícitamente o se disimule dicho contenido en el título del correo electrónico;

II. Al momento de desplegar o abrir dicho correo contenga imágenes con contenido sexual;

III. Al desplegar o abrir dicho correo contenga instrucciones para ingresar, o un mecanismo de acceso, a material con contenido sexual.

Artículo 18. Queda prohibido a toda persona promover, enviar o admitir la promoción de asuntos, negocios, bienes inmuebles, servicios, productos, ofertas de venta, rentas, arrendamientos, o cualquier otra situación que derive en un negocio mercantil, a través de un correo electrónico tipo *spam* y que contenga o esté acompañado de un título materialmente falso o engañoso para obtener una ganancia ilícita por la realización del negocio.

Artículo 19. La Comisión de Regulación del Correo Electrónico tipo *spam*, se integrará y funcionará en términos de lo que establezca el reglamento de la Ley Federal que regula al Correo Electrónico tipo *spam*. La Comisión será presidida por la Secretaría de Comunicaciones y Transportes, y tendrá entre otras las siguientes tareas:

I. Llevar un registro de todos los remitentes, reportados por los receptores, o bien descubiertos mediante cualquier medio de conocimiento, que realicen dentro de nuestro país, el envío de correos electrónicos tipo *spam*,

II. Llevar un registro de todos los remitentes que realicen envíos de correos electrónicos tipos *spam* a receptores nacionales, sean reportados o descubiertos mediante cualquier medio de conocimiento.

III. Promover a nivel nacional la cultura y participación de los usuarios de correos electrónicos en Internet, para evitar la práctica del envío de correos electrónicos tipo *spam*, así como fomentar la participación en reportar hacia la Comisión éste tipo de correos.

IV. En su caso, utilizar los avances técnicos para localizar o rastrear cualquier fuente de correo electrónico tipo *spam*.

V. Participar, coadyuvar e iniciar denuncias ante el Agente del Ministerio Público Federal, a fin de que se sancione a toda persona o compañía, que viole las prohibiciones establecidas en la presente ley.

VI. Coordinar la cooperación internacional en materia de regulación del correo electrónico tipo *spam* en los términos que fijen los Convenios y Tratados Internacionales legalmente autorizados.

VII. Recibir las denuncias o quejas respecto al correo electrónico tipo *spam*. Así como recibir las denuncias y quejas de los receptores que hayan retirado al remitente su consentimiento a recibir éste tipo de correos, y que pese a ello continúen recibiéndolos.

VIII. Vigilar, monitorear, rastrear y en su caso tomar las medidas pertinentes, dentro de los sistemas y equipos de informática del Estado, respecto del envío o recepción de cualquier tipo de correo electrónico tipo *spam*.

IX. Ser el órgano técnico, normativo y consultor en materia del correo electrónico tipo *spam*.

Artículo 20. Se equiparará al delito de Acceso ilícito a sistemas y equipos de informática, regulado por el Título Quinto, Delitos en Materia de Vías de Comunicación y Correspondencia, artículo 211 bis 1, del Código Penal Federal, y se sancionará con la misma pena que éste, a toda persona que viole cualquiera de las prohibiciones a que se refieren los artículos 6, 13, 14,15 y 16 de ésta ley.

Artículo 21. Se equiparará al delito de Fraude, regulado por el Título Vigésimo Segundo, Delitos en Contra de las Personas en su Patrimonio, en el Capítulo III, del Código Penal Federal, y se sancionará con la misma pena que éste, a toda persona que viole cualquiera de las prohibiciones a que se refieren los artículos 7, 11 y 18 de ésta ley.

Artículo 22. Se equiparará al delito de Ultrajes a la moral pública, regulado por el Título Octavo, Delitos Contra la Moral Pública y las Buenas Costumbres, Capítulo I, Artículo 200, del Código Penal Federal, y se sancionará con la misma pena que éste, a toda persona que viole la prohibición a que se refiere el artículo 17 de ésta ley.

Artículo 23. Se equiparará al delito de Falsificación de documentos en general, regulado por el Título Décimo Tercero, Falsedad, Capítulo IV del Código Penal Federal, y se sancionará con la misma pena que ésta, a toda persona que viole las prohibiciones a que se refieren los artículos 8, 9, 10 y 12 de ésta ley.

ANEXO 3. PROPUESTA DE REFORMAS Y ADICIONES A DIVERSAS DISPOSICIONES DE *LA LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR, DEL CÓDIGO PENAL FEDERAL Y DE LA LEY FEDERAL DE TELECOMUNICACIONES, EN MATERIA DE LA REMISIÓN MASIVA DE MENSAJES NO SOLICITADOS (SPAM),* PRESENTADA POR EL DIPUTADO JULIO CÉSAR CÓRDOVA MARTÍNEZ, DEL GRUPO PARLAMENTARIO DEL PRI (21 de abril de 2005).

Exposición de Motivos

El correo electrónico es en la actualidad un importante medio de comunicación para millones de mexicanos, que es utilizado diariamente para fines personales y comerciales. Su bajo costo lo ha convertido en un instrumento extraordinariamente conveniente y eficiente para desarrollar múltiples oportunidades de negocio, desarrollo y crecimiento económico.

Sin embargo, la conveniencia y eficiencia del correo electrónico se ve amenazado por el vertiginoso crecimiento del fenómeno conocido comúnmente

bajo el anglicismo de *spam*. En términos generales, aunque con variantes menores, la legislación internacional reconoce al *spam* como la remisión masiva de mensajes no solicitados que, bajo determinados supuestos legales, es considerada ilegal.

El correo *spam* también suele asociarse al llamado correo "basura". El calificativo despectivo de "basura" no necesariamente deriva de la inutilidad del mensaje, sino de su característica de remisión masiva -de forma no solicitada por sus receptores-. Entre otras posibles clasificaciones, el foro internacional reconoce dos grandes rubros de mensajes masivos (que, dados ciertos supuestos legales, pueden ser considerados como *spam):*

> Los mensajes comerciales no solicitados (*Unsolicited Commercial E-Mail, UCE*), que son mensajes con contenido publicitario; y
>
> Los mensajes no solicitados "a granel" (*Unsolicited Bulk E-Mail, UBE*), que son mensajes con contenido diverso, diferente del comercial.

Los mensajes *spam* suelen hacer presa fácil de usuarios incautos y son una amenaza a la seguridad y privacidad personales. En su inmensa mayoría, los mensajes *spam* son comunicaciones inútiles o "basura", que circulan por las redes de telecomunicaciones, con o sin destinatario, generalmente con ofrecimientos de fórmulas milagrosas para conseguir dinero fácil, logros sexuales, alertas sobre casos escandalosos, regalos o premios por reenvíos de mensajes, etcétera. En otras ocasiones, los mensajes carecen de contenido, o su contenido es inconexo o confuso. En el peor de los casos, su finalidad o efecto es causar daño o instalar programas o funciones no-deseadas en el equipo receptor o sus sistemas.

El envío de mensajes *spam* socava el valor agregado que ofrece la herramienta del correo electrónico, erosiona la confianza de los usuarios en dichas tecnologías, y evita el aprovechamiento total de los recursos y beneficios de estos medios de comunicación.

Tan sólo por citar un ejemplo, la firma estadounidense especializada en seguridad de correo electrónico Barracuda Networks ha estimado que en los últimos dos años el fenómeno de *spam* en México ha crecido al grado de abarcar el sesenta por ciento de la totalidad de correos circulantes por Internet. Esto conlleva una sobrecarga en el tráfico de las redes de comunicaciones, que incluso puede llegar a su obstrucción, así como un malgasto significativo de tiempo y recursos que son distraídos para la adquisición e implementación de mecanismos de prevención, filtro, eliminación o rechazo de mensajes *spam*.

Varias jurisdicciones ya cuentan en la actualidad con normas *antispam* para combatir, o al menos para disuadir al fenómeno. Mientras Estados Unidos de América y Australia cuentan con leyes específicas en la materia, en la Unión Europea varios países han o están ajustando sus leyes domésticas a lineamientos *antispam* derivados de dos directivas y otros instrumentos internacionales. En este último rubro cabe mencionar, de forma destacada, lineamientos dictados por la Organización para la Cooperación y el Desarrollo

Económicos (OCDE) y el foro de Cooperación Económica Asia-Pacífico (APEC) para el combate del *spam*.

Un análisis de derecho comparado revela que una legislación adecuada en materia de *spam* debe procurar el balance entre la prevención, persecución y sanción del *spam*, por un lado, y la salvaguarda de las actividades de mensajería electrónica legítima que ocurre en el curso ordinario del comercio, por el otro.

En este contexto, las normas *antispam* persiguen los siguientes objetivos básicos:

1. Definir y sancionar las actividades que constituyen *spam,* castigando con mayor severidad aquéllas cuyo propósito o efecto es causar daño a, o vulnerar la seguridad de los sistemas o equipos de informática o de tecnologías de la información, o la información contenida en ellos;

2. Dotar de mecanismos de control a los usuarios de correo electrónico sobre la recepción de mensajes;

3. Ofrecer claridad normativa para los remitentes de mensajes, que procuren el uso de medios de comunicación basados en las tecnologías de información de forma responsable; y

4. Dotar de mecanismos de control *antispam* a los proveedores de servicios de comunicaciones, así como de resarcimiento legal por el eventual daño que éstos puedan sufrir derivado del fenómeno.

La literatura y la experiencia internacionales en materia de *spam,* señala consistentemente los principales componentes deseables de una legislación *antispam,* para que ésta pueda alcanzar los objetivos antes mencionados:

1. Estrategia "antifraude" *(antifraud strategy)*. En términos generales, esta estrategia significa que la legislación *antispam* debe contener disposiciones que obliguen a los remitentes de correo electrónico a conducirse con veracidad y exactitud en la información que identifica a sus comunicaciones. El establecimiento de la obligación de identificar con veracidad y exactitud la procedencia y contenido de los correos electrónicos, es un elemento indispensable para distinguir entre la remisión de correos electrónicos legítimos, aunque ésta pueda ocurrir de forma masiva, y el *spam*.

Así pues, este tipo de disposiciones buscan cumplir los siguientes objetivos:

a) Prohibir la falsedad de los datos de identificación del mensaje (origen, procedencia, remitente, fecha, etcétera), así como los que se refieren a su contenido (indicación del asunto, texto en el contenido del mensaje). En esta categoría se incluye la práctica conocida como *spoofing,* que se refiere al uso de la extensión o el nombre de dominio de un tercero para dar la apariencia de que el correo electrónico se envía desde la cuenta

de un tercero (por ejemplo, si alguien se aprovechara del dominio de la Cámara de Diputados para aparentar que el correo lo envía alguien de la institución); y

b) Requerir información de contacto verificable. Esto significa que la información del mensaje, tanto la información de identificación inherente a él -por ejemplo, los datos de su encabezado-, como los datos proporcionados por el remitente, deben permitir el contacto real con aquél.

Un elemento secundario de la estrategia antifraude, es lo que los textos internacionales -particularmente de la literatura norteamericana- conocen como *"ADV labeling"*; algo que en español podríamos llamar "etiquetado de publicidad", o voces similares. En términos generales, este concepto guarda relación directa con los correos tipo UCE; no todos los correos comerciales no-solicitados son por sí mismos ilícitos, o pueden considerarse *spam*. Sin embargo, en la medida en que los correos comerciales no-solicitados no contengan una advertencia clara e inequívoca sobre su naturaleza, pueden ser considerados ilícitos;

2. Relaciones comerciales previas (*Preexisting business relationship, PEBR).* Este concepto se refiere a la necesidad de preservar la mensajería electrónica legítima, mediante la creación de un catálogo de supuestos "de relaciones comerciales previas", bajo los cuales los correos electrónicos, aun si son enviados de forma masiva y no solicitados, no se consideren *spam*. En realidad, el concepto de *PEBR* se ha venido ampliando en las legislaciones *antispam* de tal manera que los modelos legislativos más recientes preservan las relaciones previas entre el emisor y el receptor de un mensaje, con independencia de su naturaleza comercial;

3. Elección entre modelos legislativos de lo que se conoce como *opt-in*, u *opt-out*. Por plantearlo de una manera simplificada, el modelo de *opt-in* permite la remisión de mensajería únicamente a aquéllos destinatarios que hubieren solicitado o autorizado el mensaje. Por el contrario, el modelo de *opt-out* permite la remisión de mensajería a cualquier destinatario, siempre y cuando se le dote a dicho destinatario de una opción real de manifestar su voluntad de no continuar recibiendo mensajes del emisor, a la cuenta de correo en la cual haya sido recibido el mensaje de que se trate.

Las legislaciones más modernas del mundo en materia de tecnologías de información, reconocen el carácter deseable de un modelo de *opt-in*. Sin embargo, en la mayoría de los casos el modelo de *opt-out* ha sido el paradigma previo al modelo de *opt-in* o subsiste de alguna manera para mantener un ambiente flexible de la mensajería comercial; y

4. "Cosecha" *(harvesting).* Este elemento versa sobre la creación masiva de direcciones de correo electrónico o de usuarios en línea, para utilizarlos con fines de remisión de *spam*. De esta forma, las leyes

antispam en el mundo suelen contener normas antirrecolección de direcciones de correo electrónico o de usuarios en línea *(anti-harvesting provisions).*

También vale la pena comentar la experiencia internacional en cuanto al modelo legislativo adoptado. Mientras que Estados Unidos de América y Australia han expedido leyes especiales para combatir el fenómeno; en algunos países europeos han incorporado el concepto a las normas existentes.

Independientemente del modelo legislativo adoptado, la mayoría de las leyes *antispam* en el mundo combinan dos premisas: un catálogo limitativo de acciones que convierten a un correo electrónico en ilícito, junto con su respectivo catálogo de excepciones *(limited outright ban),* y un conjunto de normas que contengan los componentes y respondan a los objetivos planteados anteriormente.

La experiencia internacional ha demostrado que la legislación en materia de *spam* naturalmente no elimina la existencia del fenómeno; si acaso, la disuade. De hecho, países como México son aún, afortunadamente, países no generadores de un volumen significativo de *spam*. Sin embargo, el país y sus usuarios padecemos el fenómeno como un asunto de tráfico en nuestras redes de telecomunicaciones, y de distracción de tiempo, dinero y esfuerzo para filtrar y atender al *spam*.

Por otra parte, las organizaciones internacionales como la OCDE y APEC recomiendan y exhortan a sus países miembros, como es el caso de México, a llevar disposiciones *antispam* a sus leyes nacionales, para así evitar la existencia de "paraísos" para los *spammers* -quienes remiten o propagan correos *spam*- y permitir a otros países perseguir y sancionar con mayor eficacia a los grandes generadores.

En Latinoamérica, el desarrollo de legislación en la materia de *spam* es muy reciente. La legislación orientada a tecnologías de la información ha sido marcada por un claro énfasis en el desarrollo de normas en materia de firma electrónica y comercio en línea, seguido de una fase posterior en la que los países fueron identificando la necesidad de ofrecer mecanismos legales para combatir problemas derivados de la inseguridad tecnológica (delitos informáticos, pornografía infantil, entre otros). La legislación *antispam* se ubica en una tercera fase, en la que finalmente deja de percibirse al *spam* como un asunto de mero inconveniente, y se le enfrenta como un verdadero problema para la seguridad de los usuarios y la viabilidad de los medios de comunicación basados en tecnologías de la información, y el comercio electrónico.

Bajo estas premisas, someto a consideración de esta soberanía un conjunto de reformas de diversos ordenamientos, que permitan incorporar los conceptos mencionados a la legislación mexicana. El marco jurídico mexicano no es un campo virgen en la regulación de comercio electrónico o tecnologías de la información. Al menos desde 2000 nuestra legislación ha incorporado de forma importante, diversos conceptos relacionados con la materia (incluyendo, desde luego, el concepto rector de "mensaje de datos").

En este contexto, conviene aprovechar las disposiciones existentes, para dar continuidad a la tendencia legislativa que sobre la materia ha mostrado el Poder Legislativo a la fecha, al tiempo de evitar la dispersión, confusión o contradicción de conceptos que eventualmente pudiera generar la regulación en ordenamientos aislados.

Específicamente, la iniciativa plantea reformas menores en dos grandes rubros: administrativo y penal.

En el ámbito administrativo, la lógica de la iniciativa se basa en dos grandes premisas:

a) Existe un grupo de afectación constituido por los usuarios individuales de cuentas de correo electrónico o de usuarios en línea. En este grupo estamos incluidas todas las personas físicas con acceso a una cuenta de correo electrónico o de usuario en línea, que día a día somos receptores de correo no solicitado.

En relación con este sector, la iniciativa propone reglas claras y estrictas de identificación de los correos electrónicos, particularmente mercadotécnicos o publicitarios, o de contenido para adultos; así como la obligación de los emisores de incluir mecanismos mediante los cuales los destinatarios puedan ejercer efectivamente su derecho a no continuar recibiendo más mensajes de tal emisor en la cuenta de correo electrónico de que se trate.

b) Excepciones para proteger adecuadamente la remisión masiva lícita de correos electrónicos. De esta forma se asegura el balance entre la protección de la mensajería masiva lícita para preservar las relaciones de comercio electrónico, y el combate del *spam*.

La iniciativa propone que ambos supuestos, los mencionados en estos incisos, sean incorporados en la Ley Federal de Protección al Consumidor, que ya contiene disposiciones relacionadas con la materia.

Bajo la óptica penal, la iniciativa plantea la existencia de supuestos que constituyan tipos penales a incluirse en el Código Penal Federal. Esto, en relación con el concepto rector de lo que debe entenderse por un mensaje ilícito. Así, se propone que las actividades deliberadamente tendientes a la remisión de *spam* -es decir, ya no relacionadas de forma alguna con un ánimo de comercio legítimo, sino de auténtica propagación o aprovechamiento de cualquier naturaleza del o a través del *spam*- constituyan delitos. En este contexto, la iniciativa propone que, además de la inclusión de ciertos tipos penales, se acompañe de las disposiciones comunes en materia penal, referentes a la calificación del delito y la forma de reparación del daño.

Finalmente, la iniciativa propone un par de adiciones menores a la Ley Federal de Telecomunicaciones. De esta manera se incorpora el concepto en la ley de la materia para que eventualmente se permita que las autoridades relacionadas adopten medidas coordinadas o conjuntas para el combate del fenómeno.

Así las cosas, estimamos que la combinación adecuada de acciones tanto en el ámbito administrativo como en el ámbito penal, asegura la tutela de los diferentes bienes jurídicos involucrados en la materia, como lo pueden ser:

> Los derechos de los usuarios individuales;
>
> La preservación del comercio electrónico y la mensajería masiva lícita;
>
> La integridad de los servidores de los proveedores de servicios de Internet, u otros titulares de servidores "inocentes" que, por su capacidad, puedan ser utilizados para el tráfico o propagación de *spam;* y
>
> La protección de las redes públicas y privadas de telecomunicaciones.

Así, acompañada de las diversas modificaciones que ha sufrido recientemente nuestro marco legal en la materia de tecnologías de la información y comunicaciones, la presente iniciativa estima indispensable incluir en nuestro ordenamiento jurídico diversas disposiciones específicas en materia del combate al fenómeno de *spam*.

Por todo lo anteriormente expuesto, sometemos a consideración de ese Honorable Pleno de la Cámara de Diputados la siguiente

Iniciativa con proyecto de decreto que reforma y adiciona diversas disposiciones de la Ley Federal de Protección al Consumidor, del Código Penal Federal y de la Ley Federal de Telecomunicaciones, en materia de la remisión masiva de mensajes no solicitados *(spam)*

Artículo Primero. Se adicionan los artículos 17 Bis, 17 Ter, y una fracción VIII al artículo 76 Bis, y se modifica el artículo 127 de la Ley Federal de Protección al Consumidor, para quedar como sigue:

Artículo 17 Bis. Tratándose de mensajes no solicitados por el destinatario a quienes van dirigidos, enviados por correo electrónico, cada mensaje:

> I. Debe identificar clara e inequívocamente el asunto de que se trate, que permita al receptor anticipar la naturaleza y tipo de mensaje, mediante la palabra "Publicidad" o leyendas similares;
>
> II. Debe contener y operar, o permitir la operación o remitir a ella, una función de respuesta a una cuenta de correo electrónico válida y activa del remitente, o cualquier otro mecanismo basado en el Internet, que permita al destinatario manifestar su voluntad de no recibir mensajes subsecuentes en la cuenta de correo electrónico en la que se haya recibido el mensaje, salvo en los casos previstos en el artículo 17 Ter;
>
> III. No debe contener o acompañarse de información o indicaciones falsas, incluyendo la de su encabezado, que induzca al error o confusión

respecto del origen, destino, acción, asunto, fecha, hora, urgencia, tamaño o elementos adjuntos del mensaje; y

IV. No debe, en ningún caso, enviarse a través de una cuenta de correo electrónico o aprovechando el nombre de dominio de un tercero, sin consentimiento de éste.

Los mensajes no solicitados que no cumplan con los requisitos establecidos en esta ley, se considerarán ilícitos, por lo que los proveedores que sean responsables de su emisión se harán acreedores a las sanciones administrativas previstas por esta ley, sin perjuicio de cualquier otra sanción que corresponda de acuerdo con otros ordenamientos legales.

Artículo 17 Ter. El envío de mensajes no solicitados por medio de correo electrónico no dará lugar a las acciones y sanciones previstas en esta ley, en los siguientes casos:

I. Cuando el receptor tenga o haya tenido una relación comercial previa con el remitente, y el receptor no hubiere manifestado previamente al remitente su voluntad de no recibir mensajes con fines mercadotécnicos o publicitarios;

II. Cuando el receptor hubiere manifestado su aceptación o autorización para recibir mensajes por correo electrónico;

III. Cuando la recepción de mensajes por correo electrónico sea la condición que un proveedor de correo electrónico ha establecido para otorgar al usuario acceso gratuito al servicio de correo electrónico, y el usuario así lo ha aceptado;

IV. Cuando el mensaje tenga por objeto proporcionar información de garantías, de convocatorias para la atención de un determinado producto o servicio, o información de seguridad respecto de productos o servicios adquiridos previamente por el destinatario;

V. Cuando el mensaje tenga por objeto proporcionar de forma regular y periódica, información concerniente a cambios de estado, situación u otros reportes del destinatario respecto a suscripciones, membresías, cuentas, préstamos o cualesquiera otras relaciones análogas corrientes con el remitente;

VI. Cuando el mensaje tenga por objeto entregar productos o prestar servicios, incluyendo actualizaciones o mejoras a los cuales el destinatario tenga derecho de conformidad con un acto de comercio que el destinatario ha celebrado previamente con el emisor; o

VII. Cuando el mensaje tenga por objeto proporcionar información directamente relacionada con una relación de trabajo, de contrato de prestación de servicios o de derechohabiente de prestaciones o

beneficios de seguridad social, u otras relaciones reguladas por las leyes correspondientes en la materia.

Artículo 76 Bis. (...)

I. a VII. (...)

VIII. Tratándose de mensajes de datos con contenido sexual explícito o implícito, o de cualquier forma información que por su naturaleza no sea apta para menores o no esté dirigido a ellos, el emisor está obligado a incluir encabezados y leyendas claras, contrastantes y visibles que den cuenta de tal carácter, con indicaciones veraces, comprobables y exentas de textos, diálogos, sonidos, imágenes u otras descripciones que induzcan o puedan inducir al error o confusión respecto del contenido de dichos mensajes de datos, tal como **"contenido para adultos", "mensaje para adultos", "publicidad no apta para menores"** o similares.

Artículo 127. Las infracciones a lo dispuesto por los artículos 7 Bis, 13, 17, 17 Bis, 18 Bis, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 45, 47, 48, 49, 50, 52, 53, 54, 55, 57, 58, 59, 60, 61, 62, 66, 67, 68, 69, 70, 72, 75, 77, 78, 79, 81, 82, 85, 86 Quáter, 87 Bis, 90, 91, 93, 95 y 113 serán sancionadas con multa de $310.40 a $993,287.03.

Artículo Segundo. Se adiciona un Capítulo III al Título Noveno, con sus correspondientes artículos 211 Ter, 211 Ter 1, 211 Ter 2, 211 Ter 3, 211 Ter 4 y 211 Ter 5 del Código Penal Federal, para quedar como sigue:

Capítulo III
Remisión Masiva de Mensajes de Datos Ilícitos por Correo Electrónico

Artículo 211 Ter. Para los efectos del presente capítulo, los siguientes términos significan:

I. Remisión Masiva. Aquella de más de cien mensajes de datos durante un período de veinticuatro horas; más de mil mensajes de datos durante un período de treinta días, o más de diez mil mensajes de datos durante un período de un año, a cualesquiera destinatarios.

II. Encabezado. Aquellos datos de origen, destino, acción, asunto, fecha, hora, tamaño o urgencia de un mensaje de datos.

III. Mensaje de datos. Aquella información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

IV. Mensaje de Datos Ilícito:

a) Aquel que no contenga y opere, o permita la operación o remisión a ella, una función de respuesta a una cuenta de correo electrónico válida y activa del remitente, o cualquier otro mecanismo basado en el Internet, que permita al receptor manifestar su voluntad de no recibir mensajes

subsecuentes en la cuenta de correo electrónico en la que se haya recibido el mensaje, salvo en los casos previstos en el artículo 17 Ter de la Ley Federal de Protección al Consumidor;

b) Aquel que contenga o se acompañe de información o indicaciones falsas, incluyendo la de su encabezado, que induzca al error o confusión respecto del origen, destino, acción, asunto, fecha, hora, urgencia, tamaño o elementos adjuntos del mensaje;

c) Aquel que se remita a través de una cuenta de correo electrónico o aprovechando el nombre de dominio de un tercero, sin consentimiento de éste;

d) Aquel cuyo objeto o efecto sea la modificación, destrucción o pérdida transitoria o permanente, sin autorización, de todo o parte de la información contenida en sistemas o equipos informáticos, programas de computación u otros mensajes de datos, o la instalación u operación de cualesquiera tipo de programas o funciones no solicitados por el destinatario; o

e) Aquel que de cualquier forma instigue, incite, invite, cause o actualice por sí mismo la comisión de un delito u otros actos contrarios a derecho.

Artículo 211 Ter 1. Se impondrán de uno a cinco años de prisión y de ciento cincuenta a ciento cincuenta mil días multa a quien:

I. Deliberadamente realice o facilite la remisión masiva de mensajes de datos ilícitos por correo electrónico, a cualesquiera destinatarios o direcciones electrónicas;

II. Falsifique información del encabezado de cualesquiera mensajes de datos, con el objeto o efecto de realizar o facilitar la remisión masiva de mensajes de datos ilícitos por correo electrónico, a cualesquiera destinatarios o direcciones electrónicas;

III. Usando información falsa, o mediante el uso de cualesquiera mecanismos automatizados de creación, obtención, registro, identificación o envío aleatorio de cuentas de correo electrónico u otras cuentas de usuario en línea, registre o de cualquier forma obtenga cuentas de correo electrónico o cuentas de usuario en línea, o nombres de dominio, destinadas a realizar o facilitar la remisión masiva de mensajes de datos ilícitos por correo electrónico, a cualesquiera destinatarios o direcciones electrónicas, de o a través de dichas cuentas o nombres de dominio, o mediante cualquier combinación de aquéllas y éstos; o

IV. Se ostente con falsedad como titular, usuario autorizado o causahabiente legítimo de direcciones de protocolo de Internet, o direcciones IP, para realizar o facilitar la remisión masiva de mensajes de datos ilícitos por correo electrónico, a cualesquiera destinatarios o direcciones electrónicas, de o a través de dichas direcciones.

Artículo 211 Ter 2. Para la individualización de las sanciones previstas en este Título, el juez tomará en cuenta:

I. La gravedad del delito, considerando principalmente: el volumen y la naturaleza de los mensajes de datos transmitidos; el volumen de cuentas de correo electrónico, de usuario en línea, de nombres de dominio o de direcciones de Protocolo de Internet o direcciones IP involucradas, y los daños causados a terceros;

II. La comisión de conductas delictivas u otros actos ilícitos en violación a sistemas o equipos informáticos, programas de computación o mensajes de datos;

III. Las condiciones económicas de quien comete el delito;

IV. La reincidencia, si la hubiere; y

V. El beneficio directamente obtenido por quien comete el delito o por terceros, si lo hubiere.

Artículo 211 Ter 3. Los delitos previstos en el presente capítulo se perseguirán por querella de parte ofendida. Es parte ofendida el titular de los sistemas o equipos de informática, programas de computación o mensajes de datos que, sin su autorización, sean usados o de cualquier forma aprovechados para realizar o facilitar la remisión de mensajes de datos ilícitos por correo electrónico conforme a lo previsto en el presente capítulo.

Artículo 211 Ter 4. Las sanciones pecuniarias previstas en el presente capítulo se aplicarán sin perjuicio de la reparación del daño, cuyo monto no podrá ser menor a la cantidad más grande entre:

I. El daño patrimonial causado a la parte ofendida; y

II. La cantidad que resulte de multiplicar el número de mensajes de datos ilícitos remitidos de o a través de los sistemas o equipos informáticos de la parte ofendida, por trece días de salario mínimo vigente en el Distrito Federal, sin que pueda exceder a la cantidad equivalente a doscientos sesenta mil días de salario mínimo vigente en el Distrito Federal.

Artículo 211 Ter 5. Los prestadores de servicios de telecomunicaciones o de servicios de valor agregado, incluyendo a los proveedores de servicios de Internet o de correo electrónico, no son responsables de forma alguna por la transmisión de cualesquiera mensajes de datos a través de sus sistemas o equipos de informática o redes de telecomunicaciones, en la medida en que dicha transmisión esté basada en la información que sobre el receptor o destinatario provea el usuario del servicio o un tercero.

Artículo Tercero. Se adiciona un segundo párrafo al artículo 70 y se adiciona una fracción VI al apartado A del artículo 71 de la Ley Federal de Telecomunicaciones, para quedar como sigue:

Artículo 70. (...)

La Secretaría ejercerá las acciones que procedan para prevenir, corregir o sancionar cualesquiera perturbaciones a las redes, sistemas o servicios de telecomunicaciones, o a sistemas o equipos de informática relacionados con ellos, incluyendo la negación del servicio, derivado de la realización o facilitación de la remisión masiva de mensajes de datos ilícitos por correo electrónico.

Artículo 71. (...)

A. (...)

I. a V. (...)

VI. Realizar o facilitar la remisión masiva de mensajes de datos ilícitos por correo electrónico, en perjuicio de los sistemas o servicios de telecomunicaciones, o de sistemas o equipos informáticos de cualesquiera concesionarios o permisionarios. Son mensajes de datos ilícitos los que así se clasifiquen en términos del artículo 211 Ter del Código Penal Federal.