INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE MONTERREY

ESCUELA DE GRADUADOS EN ADMINISTRACIÓN PÚBLICA Y POLÍTICA PÚBLICA, CAMPUS CIUDAD DE MÉXICO

Regulación Jurídica del Correo Electrónico No Deseado (*Spam)*

Lic. Sonia María Lazcano Romero
ITESM-CCM
daso6@hotmail.com

Proyecto de Investigación Aplicada
Maestría en Derecho Internacional
Asesor: Dr. Julio Téllez Valdés
Diciembre de 2005

Índice

Resumen Ejecutivo

Con el auge del comercio electrónico surgen prácticas nocivas hacia los usuarios de internet y que día a día atacan su intimidad. Podemos decir, que una de esas prácticas es el surgimiento del correo electrónico no deseado denominado en la Sociedad de la Información e internet como *Spam*, mismo que ha ido en aumento en los últimos años.

Para conocer el origen de esta práctica, se presentará en un primer capítulo la relevancia que tiene el comercio electrónico como sus principales ventajas y desventajas, enfatizando como una de estas últimas, el uso del correo electrónico cuando es utilizado, para los envíos masivos de correos que no fueron solicitados por los receptores.

Teniendo a continuación un segundo capítulo dedicado al *Spam*, en el cual se detallará su origen y su falta de definición homogénea en el entorno internacional, sus clases, puntualizando el impacto que tiene el correo no solicitado en las practicas comerciales en línea, en la propiedad intelectual de la información y en la protección de datos personales de los usuarios.

En un tercer capítulo, se analizará la regulación jurídica internacional de este fenómeno, a través del estudio de las principales legislaciones que han sido detonantes para que otros países las adopten o bien para crear las suyas, y acuerdos internacionales que sugieren la cooperación mundial para el combate antispam.

La última parte de esta investigación, abarcará las acciones que se llevan a cabo en México a través de determinadas autoridades, como la poca protección que existe para esta práctica, por lo que también se presentará las propuestas legislativas que tratan de regular la materia de correo electrónico no solicitado, y que se encuentran pendientes de aprobación en el Pleno de la Cámara de Diputados.

Introducción

La tecnología ha permitido el desarrollo económico y social del mundo, siendo un detonador para el mejoramiento de las prácticas comerciales internacionales, creando una herramienta que permite el intercambio de los diferentes tipos de bienes y servicios de una forma más ágil y a bajos costos, nos referimos a Internet, que ha motivado el surgimiento y crecimiento de una nueva forma de hacer comercio: *comercio electrónico o e-commerce*.

Dentro de este comercio, se tiene como estrategia principal el envío de publicidad a través de la web para llegar a los consumidores y con ello incrementar las utilidades, pero encontramos que no toda la publicidad que se envía es veraz y que hoy en día ha proliferado la publicidad nociva y engañosa, por medio de la cual solo un determinado grupo de personas se enriquecen a costa del envío de mensajes no solicitados a los usuarios o consumidores en línea.

Estos mensajes denominados como correos electrónicos no deseados, entre otras cosas han traído la lentitud de la red, grandes pérdidas económicas a nivel internacional y la pérdida de tiempo de los usuarios, ocasionando la baja en la productividad de las empresas y de los particulares.

Así mismo estos mensajes, abarcan aproximadamente el setenta por ciento de los correos electrónicos que hay en la red, y su contenido en la mayoría de las ocasiones se utilizan para defraudar al consumidor a través de engaños como son el solicitarle depósitos de determinadas cantidades de dinero para apoyar alguna causa con la promesa de que se hará acreedor a una jugosa indemnización económica, o bien la compra de productos con características milagrosas para la cura de alguna enfermedad o peor aun, el contenido de estos mensajes puede ser pornográfico o no apto para los menores, ocasionando daño a la moral y a la comunidad en general.

A través de esta práctica, los usuarios reciben mensajes de remitentes con los que nunca se ha tenido relación alguna, violándose el derecho a la privacidad de datos personales o confidenciales de los usuarios como lo es la cuenta de correo electrónico. Por lo anterior, resulta de suma importancia abordar este tema, para conocer en detalle los alcances del *Spam,* y las acciones que se han desarrollado como posibles medios de eliminarlo o disminuirlo, para lograr la confiabilidad en las practicas comerciales en línea y por consiguiente su crecimiento global, por lo cual el presente proyecto de investigación se desarrollará de la siguiente manera:

En el capítulo primero se presentan las generalidades del comercio electrónico, así como sus características, puntualizando las implicaciones positivas y negativas que trae consigo este comercio, señalando los principales servicios que se ofrecen a los usuarios a través de internet, especificando su regulación jurídica en el contexto internacional y nacional.

En el capítulo segundo, abordaré el origen y evolución del servicio de correo electrónico, con la finalidad de delimitar el surgimiento del correo electrónico no solicitado o *Spam* tema central del presente proyecto. Para lo cual, se detallarán sus características, clases y ejemplos más comunes que circulan en la web, mencionando el impacto económico ocasionado por esta tipo de correo y se llevará a cabo un análisis de la regulación jurídica en materia de protección de datos personales y propiedad intelectual de la información.

El capítulo tercero, contiene los instrumentos jurídicos creados para el combate en contra del correo tipo *Spam* más sobresalientes en países como Estados Unidos de América, España y la Unión Europea, así como las acciones internacionales que a la fecha se han alcanzado para hacer frente a esta problemática.

En el último capítulo se revisarán las medidas con las que se cuentan por parte de algunas autoridades en México, junto con organismos internacionales para el combate antispam, y la poca regulación jurídica que existe en esta materia, revisando las propuestas de reformas y de iniciativa de ley que han sido presentadas en el Congreso de la Unión,

enfatizando la necesidad que se regule esta práctica y que se ofrezca ciberseguridad a los usuarios de internet en nuestro país.

Objetivos Generales:

El presente proyecto de investigación tiene tres objetivos fundamentales:

1.- Analizar la repercusión nacional e internacional del correo electrónico no deseado, conocido en la Sociedad de la Información e internet como *Spam*.

2.- Demostrar las repercusiones que trae consigo este tipo de correo en el contexto del comercio electrónico.

3.- Lograr que nuestros legisladores pongan en marcha medidas jurídicas para el combate contra esta práctica nociva y la protección al derecho a la privacidad de los usuarios de internet, para contrarrestar la inseguridad jurídica que existe en las prácticas comerciales que se llevan a cabo en línea.

Objetivos Específicos:

1.- Delimitar el origen y definición del correo publicitario no deseado, así como el impacto de este correo en las transacciones comerciales internacionales en línea.

2.- Determinar el daño que sufre la privacidad de datos personales y la sociedad en general en virtud de la práctica del *Spam*.

3.- Demostrar la importancia que tiene contar con una regulación nacional para combatir el correo no solicitado, en virtud del crecimiento que presenta este correo y las grandes pérdidas económicas para los usuarios y para los prestadores de servicios de internet.

enfatizando la necesidad que se regule esta práctica y que se ofrezca ciberseguridad a los usuarios de internet en nuestro país.

Objetivos Generales:

El presente proyecto de investigación tiene tres objetivos fundamentales:

1.- Analizar la repercusión nacional e internacional del correo electrónico no deseado, conocido en la Sociedad de la Información e internet como *Spam*.

2.- Demostrar las repercusiones que trae consigo este tipo de correo en el contexto del comercio electrónico.

3.- Lograr que nuestros legisladores pongan en marcha medidas jurídicas para el combate contra esta práctica nociva y la protección al derecho a la privacidad de los usuarios de internet, para contrarrestar la inseguridad jurídica que existe en las prácticas comerciales que se llevan a cabo en línea.

Objetivos Específicos:

1.- Delimitar el origen y definición del correo publicitario no deseado, así como el impacto de este correo en las transacciones comerciales internacionales en línea.

2.- Determinar el daño que sufre la privacidad de datos personales y la sociedad en general en virtud de la práctica del *Spam*.

3.- Demostrar la importancia que tiene contar con una regulación nacional para combatir el correo no solicitado, en virtud del crecimiento que presenta este correo y las grandes pérdidas económicas para los usuarios y para los prestadores de servicios de internet.

Marco Teórico

El desarrollo teórico del presente proyecto de investigación, se basa en la revisión y análisis de la bibliografía existente a partir del surgimiento del correo electrónico no solicitado *Spam*, desarrollada por las distintas organizaciones internacionales, como la Organización para la Cooperación y el Desarrollo Económico (OCDE), Unión Internacional de Telecomunicaciones (UIT) a través de Organización de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), Organización Mundial del Comercio (OMC), Organización Mundial de la Propiedad Intelectual (OMPI), Red Internacional de Protección al Consumidor y de Aplicación a la Ley (International Consumer Protection and Enforcement Network ICPEN), y de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional de la Organización de las Naciones Unidas (ONU) principalmente, así como la doctrina desarrollada sobre este tema tanto a nivel nacional como internacional.

De igual manera se realizó en la investigación, el análisis de las legislaciones en materia de correo electrónico no solicitado que han tenido una mayor repercusión como es la CAN SPAM Act, (Ley Federal vigente de Estados Unidos de Norteamérica) y la Ley Estatal de California, Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico de España y la Directiva de la Unión Europea 2002/ 58/CE, como de la legislación mexicana existente en esta materia.

Por la naturaleza del tema se ha consultado información contenida en numerosos sitios web, mismos que se citan en la bibliografía, complementando la investigación a través del análisis de estadísticas, notas periodísticas sobre el tema y de la entrevista realizada al Director Jurídico de Microsoft México.

Marco Metodológico

La clase de investigación se basa primero en estudios exploratorivos, que logran definir el problema para determinar la orientación y el sentido de la investigación, con la finalidad de lograr el conocimiento de la realidad que se esta investigando con el apoyo de estadísticas, entrevista y de notas periodísticas que demuestran la hipótesis de investigación.

Asimismo, tiene como fundamento metodológico el análisis comparativo de las distintas legislaciones internacionales y nacionales existentes, para identificar y determinar las variables que versan sobre los daños ocasionados a la sociedad de la información en general por el envío de correos no solicitados y que utilizando el método deductivo a partir de la investigación del comercio electrónico se logra llegar a la problemática particular que es el *Spam.* Una vez delimitado este fenómeno particular, se utilizará el método inductivo para llegar a conclusiones generales.

Capítulo I Comercio Electrónico

1. Generalidades

A través del los tiempos, el comercio ha sido de gran utilidad para el hombre, ya que ha permitido el crecimiento económico de la sociedad con el intercambio de bienes y servicios en forma local así como con otros países, indudablemente ha sido el gran motor para la creación de medios que lo faciliten, como es el caso de los medios de transporte, la tecnología, las telecomunicaciones, entre otros.

A partir de las últimas décadas del Siglo XX, con la creación de la red de redes (internet), se abren nuevas posibilidades para el comercio, con la incorporación de medios electrónicos dando lugar al surgimiento de lo que hoy conocemos como comercio electrónico, provocando una revolución en la nueva forma de hacer comercio a nivel internacional.

Por medio del comercio electrónico, surgen nuevas transacciones como contratos electrónicos, servicio de correo electrónico, pagos por vía electrónica, etc., prácticamente agiliza las operaciones eliminando costos y tiempo de operación entre los actores que intervienen en el (proveedores, consumidores e intermediarios), esto ha permitido que en la actualidad desde cualquier parte del mundo y a cualquier hora, podamos tener a nuestro alcance toda una gama de mercancías y servicios, como serían la producción, publicidad, venta y distribución de bienes a través de las redes de telecomunicaciones.

El comercio electrónico, ha traído consigo una gran repercusión en la vida económica, social, tecnológica y jurídica del mundo, y conforme se ha ido desarrollando surgen nuevas herramientas y protecciones para el mismo, ya que además de que permite tener una mejor comunicación entre los individuos y, como anteriormente señalo, una agilidad para hacer

comercio por lo que surgen nuevos problemas de seguridad que en el panorama nacional e internacional no ha sido del todo resuelto.

2. Definición

Para delimitar un concepto de comercio electrónico, partiré del análisis de los componentes que lo integran:

De acuerdo al Real Academia Española[1] tenemos que *Comercio*: (Del lat. *commercĭum*). 1. m. Negociación que se hace comprando y vendiendo o permutando géneros o mercancías. Y por *Electrónico:* (De *electrón* e *–ico*). 2. adj. Perteneciente o relativo a la electrónica.

~ electrónico.1. m. Sistema de comunicación por ordenador a través de redes informáticas.

Combinando estos dos términos podemos esbozar una definición gramatical del comercio electrónico diciendo que es la negociación que se hace comprando y vendiendo o permutando géneros o mercancías utilizando un sistema de comunicación por ordenador a través de redes informáticas.

Por medio de estas redes, se permite el procesamiento de datos, imágenes, videos entre otros, teniendo dos tipos de redes:

1. Red privada: Es la que operan para propósitos específicos y están destinados exclusivamente para participantes autorizados,

2. Red abierta: Es la que opera con dispositivos de seguridad y permite que un número ilimitado la usen.[2]

[1] Diccionario Real Academia Española. 22.ª Ed., 2001 http://biblioteca.itesm.mx/nav/contenidos_salta2.php?col_id=drae (Sept 5,2005)
[2] Téllez Valdés, Julio. *Derecho informático.* 3ª. Ed. México, McGraw Hill, 2004. p. 186

Para ejemplificar ambas redes, tenemos como redes privadas a bases de datos de clientes e Intranet, y que lo realizan a través del medio denominado *Electronic data interchange* (EDI).

En cuanto a redes abiertas encontramos a Internet, que utiliza un protocolo denominado Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP), y emplea un sistema de codificación, el lenguaje de marcación de hipertexto (HTML), a través del cual se puede representar datos en la World Wide Web (WWW), transmisión de archivos (FTP) y correo electrónico (e-mail) principalmente.

Asimismo la World Trade Organization (WTO) lo define como: "La producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos"[3].

Tomando en consideración la diversificación en cuanto a términos se refiere, esto hace difícil la creación de una definición universalmente aceptada del Comercio Electrónico, ya que muchos autores u organizaciones han mantenido una discrepancia para delimitar dicho concepto, por lo que para una mejor comprensión y de acuerdo a Andrea Viviana Sarra, mencionare las modalidades de este tipo de comercio así como sus diferencias con el objeto de definirlo:

1) El comercio electrónico directo: Que se lleva a cabo íntegramente por vía electrónica.
2) El comercio electrónico indirecto: Que se realiza mediante pedidos de bienes y servicios tanto materiales como intangibles a través de las redes, pero que se suministran por medio de los canales normales de distribución física.

[3] Declaración sobre el Comercio Electrónico Mundial adoptada por los Ministros en el segundo período de sesiones de la Conferencia Ministerial del 25 de septiembre de 1998. http://www.wto.org/spanish/tratop_s/ecom_s/wkprog_s.htm (Sept. 13, 2005)

En la tabla siguiente se muestran las diferencias entre dos componentes del comercio electrónico: el tradicional y el que utiliza un entorno de redes abiertas:[4]

Comercio Electrónico Tradicional	*Comercio Electrónico en entorno de redes abiertas (Internet)*
Transferencia Electrónica de fondos	Transferencia Electrónica de fondos
Transacciones o Acuerdos vía correo electrónico	Transacciones o Acuerdos vía correo electrónico
Tarjetas inteligentes	Tarjetas inteligentes
Sistemas de gestión por *workflow* EDI	Sistemas de gestión por *workflow* EDI
Venta por catálogo en CD-ROM	Venta por catálogo en CD-ROM
Intranets	Comercialización digital de bienes y servicios
	Compraventa de acciones digitalmente
	Conocimientos de embarques electrónicos
	Suministro en línea de contenidos digitales
	Subastas
	Diseños y productos conjuntos
	Prestación de servicios en línea
	Contratación pública
	Comercialización directa al consumidor
	Servicios de postventa
	Telecompras
	Catálogos en CD-ROM con conexión a Internet
	Infomercials con mecanismos de respuestas a través de la red
	Sitios *web* con extensiones en CD-ROM para demostraciones en multimedia

[5]

[4] El comercio electrónico tradicional es aquel en el que se utilizan las redes para transmitir datos, por ejemplo datos de mercados cautivos; por su parte el que utiliza un entorno de redes abiertas (internet) las redes vienen a ser el mercado no solo trasportadoras de datos.

[5] Sarra, Andrea V. *Comercio electrónico y derecho*. Buenos Aires, Astrea, 2000. p. 285

Por todo lo anterior el comercio electrónico, es aquel que permite la realización de transacciones comerciales a través de redes abiertas o cerradas.

En la práctica comercial, encontramos, varios sinónimos de comercio electrónico como son: e-business, m-business (porque utiliza comunicaciones inalámbricas) y el término de e-commerce.

Dentro de este comercio encontramos varios tipos como son:

1. B2B (Business to business): El cual esta dirigido a las operaciones entre empresas. Por ejemplo las operaciones que se realizan entre fabricantes y comercializadores.
2. B2C (Business to Consumer): El cual esta dirigido a las operaciones entre empresa y consumidor. Por ejemplo el Mercado Libre por Internet.
3. B2A (Business to Administration): El cual esta dirigido a las operaciones entre empresa y Administración Pública. Por ejemplo Compranet.

Por lo que podemos determinar que los actores que intervienen en el mismo son: Las empresas, los consumidores y la Administración Pública.

3. Características

El auge que tiene el comercio electrónico, es en gran medida por que facilita las operaciones comerciales: uno por sus bajos costos y dos por el factor tiempo de realización.

Siendo así, el comercio no es exclusivo de las grandes corporaciones, sino también de las PyMES (Pequeñas y Medianas empresas) y de los particulares, ya que lo utilizan cada vez más para acercar sus productos a nivel nacional e internacional.

Cabe destacar que ningún medio como lo es internet, se había desarrollado tan vertiginosamente[6] y ha llegado cada vez más a los consumidores; gracias a esta Red podemos conocer bienes de carácter intangible y cada vez más se suman operaciones a realizar.

Encontramos operaciones como contratos electrónicos, pagos electrónicos, publicidad, conocimientos de embarque, trámites administrativos (como lo es la Facturación Electrónica Avanzada o Fiable), comunicación, búsqueda de información, venta de software, de música, de libros o bien desde nuestro domicilio podemos contratar viajes, eventos, etc., y con estas se ha propiciado un desarrollo económico y tecnológico sin fin.

Asimismo es muy importante el factor confianza por parte de los actores que intervienen ya que siendo en su mayoría bienes intangibles, el consumidor al comprar un bien, deposita su confianza para pagar y recibir el producto o servicio, mientras que por parte del proveedor deberá de generarla para poder permanecer en el mercado e incluso para incrementarlo. Al efecto se ha desarrollado otro tipo de derechos como lo es la propiedad intelectual y convenios internacionales, así como la creación de instituciones certificadoras para dar apoyo a las operaciones de e-commerce, pero esto no ha sido suficiente por lo que este tema lo abordaré más adelante.

Con lo anterior, se puede determinar que las principales características del comercio electrónico son:

1. Es un comercio que implica poca inversión.
2. Poco tiempo de operación.
3. Acercamiento cada vez mayor hacia los consumidores.
4. Amplia gama de transacciones comerciales.
5. Confianza.

[6] El número de usuarios Internet, que según las estimaciones de la UIT es de unos 700 millones (lo que representa cerca del 11% de la población mundial).ITU (Internacional Telecommunications Union). http://www.itu.int/newsroom/press_releases/2005/05-es.html (Sept. 13,2005)

4. Implicaciones Positivas y Negativas

Tomando en cuenta las características antes mencionadas, podemos determinar como implicaciones positivas:

a) Acceso fácil a la red y con ello acceso a la información y comunicación.
b) Disminución de barreras comerciales entre países.
c) Crecimiento en las producciones y en la tecnología.
d) Amplía el conocimiento del consumidor provocando que las empresas oferten con mayor calidad y que estas sean más eficaces, además esto ha permitido también que cada vez menos intervengan los intermediarios en la cadena comercial.
e) Reducción de costos.

Pero no todo ha sido bueno en este tipo de comercio, ya que ha traído consigo problemas de relevancia jurídica, tecnológica y social. Aunque es cada vez mayor el alcance de los particulares a los sistemas de información aun quedan muchas regiones por abarcar. Además, tenemos que no todo lo que encontramos en Internet es de calidad y del todo seguro, propiciando el crecimiento de ilícitos en la red, siendo los más comunes:

a) La difusión de instrucciones sobre preparación de bombas, las actividades terroristas, la producción y tráfico de drogas, y el activismo político, lo que atenta en contra de la seguridad nacional y mundial;
b) La oferta de servicios sexuales y pornografía relacionada con niños (pedofilia), lo que requiere velar por la protección de menores;
c) El envío de mensajes que incitan al odio y la discriminación racial o religiosa, lo que atenta contra la dignidad humana;
d) Las conductas de hurto y destrucción de datos que realizan los *hackers*[7], que atentan contra la seguridad y confidencialidad de la información;

[7] Además de los *Hacker*s o piratas que son los que gozan alcanzando un conocimiento profundo sobre el funcionamiento interno de un sistema, de una computadora o de una red de computadoras, también

e) Los delitos de "piratería" de software, que vulneran la propiedad intelectual;

f) El mal uso de tarjetas de crédito ajenas, lo que atenta contra la seguridad económica;

g) La recolección, procesamiento y transmisión no autorizada de datos personales, lo que requiere proteger legalmente la privacidad o intimidad de las personas

h) El envío de mensajes difamatorios o injuriantes, lo que atenta contra la honra y dignidad de las personas; y

i) La publicación o inclusión de hipervínculos a rutinas de desencriptación de sistemas de protección de contenidos como ser la rutina que protege el sistema de reproducción de DVD.[8]

Con todo lo anterior, existe un gran campo de acción para contrarrestar la problemática que se presenta en este entorno, requerimos de una mayor protección de leyes nacionales e internacionales, así como el mejoramiento de la tecnología para hacer más seguro el uso de la red.

5. Regulación Jurídica del Comercio Electrónico

En el ámbito internacional en cuanto al comercio electrónico se refiere, tenemos a La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) y por sus siglas en ingles (UNCITRAL), establecida por la Asamblea General en 1966. La Asamblea General, al establecer la Comisión, reconoció que las disparidades entre las leyes nacionales que regían el comercio internacional creaban obstáculos para ese comercio, y

---

encontramos otro tipo como los son los *Crackers* o saboteador que es el que intenta acceder (con mala intención) a un sistema informático sin autorización y *Phracker* o fonopirata quien es un pirata informático especializado en utilizar redes telefónicas para acceder a sistemas ajenos o a menudo solo para evitar pagar las facturas telefónicas. Téllez, Op. Cit. pp. 457, 470 y 489.

[8] Jijena L., Renato; Palazzi, Pablo A. y Julio Téllez V. *El Derecho y la Sociedad de la Información: la importancia de Internet en el mundo actual*. México, Miguel Ángel Porrúa y Tec de Monterrey, Campus Estado de México. 2003. pp. 51 y 52

consideró que, mediante la Comisión, las Naciones Unidas podrían desempeñar un papel más activo en la reducción o eliminación de esos obstáculos[9].

La Asamblea General dio a la Comisión el mandato general de fomentar la armonización y unificación progresivas del derecho mercantil internacional. Desde entonces, la Comisión se ha convertido en el órgano jurídico central del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional, y es este organismo quien crea la Ley Modelo sobre el Comercio Electrónico el 16 de Diciembre de 1996, la cual tiene como objeto facilitar el uso del comercio electrónico a nivel internacional y es aplicable a toda aquella información que sea por medio de mensaje de datos[10] utilizada en las actividades comerciales (transporte de mercancías, intercambio de información, contratos, por ejemplo).

Asimismo, da validez y fuerza probatoria a cualquier medio digital, y establece que cuando la ley requiera información esta deberá ser conservada en su forma original y podrá ser presentada a través de un mensaje de datos. Colabora con los Estados para ingresar a su Derecho Interno la incorporación de esta Ley.

Por su parte la Organización para la Cooperación y el Desarrollo Económico(Organisation for Economic Co-operation and Development OECD), en la Recomendación del Consejo, relativa a los Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico, aprobado el 9 de Diciembre de 1999, establece como su objetivo principal la protección transparente y efectiva a todos los usuarios en línea, estableciendo que las empresas que realicen actividades de mercadeo o publicidad, deberán respetar los intereses de los consumidores, también señala la obligación de proporcionarles información sobre ellas mismas y de los bienes o servicios que oferten, así como las condiciones, términos y costos de los mismos en forma precisa y guardar la

[9] "Origen, mandato y composición" 2005. http://www.uncitral.org/uncitral/es/about/origin.html (Oct. 18, 2005)

[10] Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax. Véase "A/RES/51/162" s/f, http://www.un.org/spanish/documents/ga/res/51/list51.htm (Oct.18, 2005)

privacidad de las operaciones que realicen. En el marco de la OECD, se respeta el derecho interno de cada país, estableciendo este marco internacional, para promover, incorporar y fomentar la protección al usuario.

En el 2003, publicó la Resolución sobre los Lineamientos para proteger a los consumidores de prácticas comerciales transfronterizas, fraudulentas y engañosas, en donde se pretende combatir las transacciones de este tipo entre las empresas y consumidores (*B2C: Business to Consumer*), incluyendo a los Estados miembros y a los no miembros.

Dentro del marco jurídico mexicano han sido recientes las modificaciones o adhesiones que se han realizado para el comercio electrónico, ya que fue a partir del año 2000 que se hicieron reformas en el Código Civil Federal (1, 1803, 1805 y 1811, y se le adiciona el artículo 1834 bis), Código Federal de Procedimientos Civiles (se adiciona el artículo 210-A), Código de Comercio (Se reforman los artículos 18, 20, 21 párrafo primero, 22, 23, 24, 25, 26, 27, 30, 31, 32, 49, 80 y 1205, y se adicionan los artículos 20 bis, 21 bis, 21 bis 1, 30 bis, 30 bis 1 y 32 bis 1298-A; el Título II que se denomina "Del Comercio Electrónico", que comprende los artículos 89 al 114, Vigente a partir del 27 de Noviembre de 2003, y se modifica la denominación del Libro Segundo de dicho Código) y a la Ley Federal de Protección al Consumidor (Se reforma el párrafo primero del artículo 128, y se adiciona la fracción VIII al artículo 1°, la fracción IX bis al artículo 24 y el Capítulo VIII bis, que contiene el artículo 76 bis), de las cuales mencionare los puntos más importantes:

1. Código Civil Federal

En el consentimiento de los actos jurídicos, se adiciona que este también podrá realizarse a través de medios electrónicos, ópticos o por cualquier otra tecnología, además de los que anteriormente aceptaba (Expreso: verbal, escrito o por signos inequívocos y Tácito: que es aquel consentimiento que resulta de hechos o actos que lo presuman).

En cuanto a la figura de la oferta estipula el Código, si esta la hace el autor de la oferta a una persona presente, si no hay una aceptación inmediata, el autor quedará desligado, el mismo supuesto se aplica cuando se hace por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología por la que se haya manifestado la oferta. Asimismo estas dos figuras tanto la oferta como la aceptación por medios electrónicos producen todos sus efectos, sin estipulación previa entre los contratantes.

También hace referencia a la forma de los contratos, señalando que cuando se exija que estos deban constar por escrito y firmados por las partes, se pueden utilizar los medios electrónicos, ópticos o de cualquier otra tecnología, siempre y cuando se proporcionen todos los datos en forma íntegra, es decir, los contratantes pueden generar, enviar, recibir, archivar o comunicar los términos en que se obligaron en el contrato. Si se requiere que se celebre ante algún Fedatario Público, se podrá también hacer por estos medios, haciendo constar el Fedatario el medio por el cual se celebró el contrato y guardará una copia fiel de ese medio.

2. Código Federal de Procedimientos Civiles

Reconoce como prueba aquella información que haya sido generada o informada a través de los medios electrónicos, ópticos o en cualquier otra tecnología. Para que esta tenga fuerza probatoria se tendrá que demostrar que el medio que la generó es fiable, señalar a las personar responsables del contenido (si es posible) y conservar un original íntegra e inalterada de la información (en el medio en que se utilizó), y que esta pueda ser accesible para ser consultada.

3. Código de Comercio

Las modificaciones a este ordenamiento guardan una fundamental relevancia en el entorno del Comercio Electrónico, ya que este incluye un Título para este comercio y contempla nuevas figuras dentro del derecho mercantil mexicano, como son:

Titulo II DEL COMERCIO ELECTRONICO

Artículo 89: En los actos de comercio podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología, establece las siguientes definiciones:

Certificado: Todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de firma electrónica.

Datos de creación de firma electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el firmante genera de manera secreta y utiliza para crear su firma electrónica, a fin de lograr el vínculo entre dicha firma electrónica y el firmante.

Destinatario: La persona designada por el emisor para recibir el mensaje de datos, pero que no este actuando a titulo de intermediario con respecto ha dicho mensaje.

Emisor: Toda persona que, al tenor del mensaje de datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si este es el caso, pero que no haya actuado a titulo de intermediario.

Firma Electrónica (FE): Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Firma Electrónica Avanzada o Fiable: Aquella firma electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.

En aquellas disposiciones que se refieran a *firma digital*, se considerará a esta como una especie de la firma electrónica.

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario: En relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él.

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

Parte que confía: La persona que, siendo o no el destinatario, actúa sobre la base de un certificado o de una firma electrónica.

Prestador de servicios de certificación: La persona o institución pública que preste servicios relacionados con firmas electrónicas y que expide los certificados, en su caso.

Secretaria: Se entenderá la Secretaria de Economía.

Sistema de información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Titular del certificado: Se entenderá a la persona a cuyo favor fue expedido el certificado.

Asimismo, estas reformas establecen la automatización del Registro Público del Comercio, en el cual se inscriben los actos mercantiles a través del programa informático, y reconoce como medios de prueba a los mensajes de datos.

4. Ley Federal de Protección al Consumidor

En esta ley se establece la protección de la información del consumidor y promueve que los proveedores o empresas que utilicen información sobre consumidores, no utilicen la misma con fines distintos a los mercadológicos ó publicitarios. Esta ley la analizaré más

adelante, en virtud de que sus disposiciones conllevan a la materia de la investigación que aquí se presenta.[11].

Junto con estas reformas ha surgido la necesidad de que en otras áreas del derecho se contemplen nuevas disposiciones en virtud de la creación de estas nuevas figuras, así como del crecimiento de las nuevas operaciones comerciales, tal es el caso de la materia fiscal y bancaria.

El Código Fiscal de la Federación, establece disposiciones sobre los Medios Electrónicos como lo son la Firma Electrónica Avanzada o Fiable así como la Facturación Electrónica[12], y dispone:

Cuando las disposiciones fiscales obliguen a presentar documentos estos deberán ser digitalizados y contener una firma electrónica avanzada del autor.

Esta Firma Electrónica Avanzada o Fiable:

1. Sustituirá a la firma autógrafa del firmante.
2. Garantizará la integridad del documento y producirá los mismos efectos que las leyes otorgan a los documentos con firma autógrafa.
3. Tendrá el mismo valor probatorio.

En cuanto a la facturación, determina la obligatoriedad de entregar Factura Electrónica por parte de los proveedores y empresas, y establece un sistema de certificación a través del Sistema de Administración Tributaria (SAT), el cual esta contemplado en el Reglamento de este ordenamiento. Pero para este sistema aun quedan muchas lagunas ya que no es claro y en México no se cuenta con el sistema de soporte para las operaciones, por lo que no se puede definir aún una autentica automatización en las operaciones comerciales.

[11] Vid supra. Capítulo IV
[12] Vigente a partir del 1ro. de Enero del 2005.

Hoy en día, los contribuyentes pueden presentar su declaración fiscal vía electrónica, pero aun se enfrentan con problemas de carácter tecnológico y resulta en ocasiones difícil de elaborar o enviar a la autoridad.

Por último, tenemos a la Ley de Instituciones de Crédito, la cual establece que las operaciones y la prestación de servicios al público la podrán realizar a través del uso de equipos, medios electrónicos, ópticos o de cualquier otra tecnología, sistemas automatizados de procesamiento de datos y redes de telecomunicaciones, ya sean privados o públicos, como por ejemplo *BancaNet.*

Estas operaciones siguen los lineamientos que establece la Comisión Nacional Bancaria y de Valores (CNBV), y entre otras operaciones que podemos realizar tenemos: Pagos electrónicos, depósitos, consulta de saldos, inversiones, etc. a través de los medios de identificación del usuario.

Todas estas reformas, se ven apoyadas por otros reglamentos, acuerdos y NOMs (Normas Oficiales Mexicanas), correspondientes a cada una de estas materias del derecho.

En forma general, podemos decir que aunque es reciente el comercio electrónico en nuestro derecho y a pesar de las reformas aquí descritas, esto no es suficiente, ya que hay puntos como la protección al usuario, que no cuenta con alguna regulación, por lo que en especial abordaré este tema a continuación.

Capítulo II Correo Electrónico No Deseado *"Spam"*

1. Correo Electrónico: Antecedentes y Evolución

A partir del surgimiento del ARPANET (*Advanced Research Projects Agency Network*), creada por el Departamento de Defensa de los Estados Unidos de América en tiempos de la Guerra Fría, y cuya finalidad era tener una red que contuviera información en paquetes (Fragmentar información y dividirla en determinadas porciones y enviarla hacia su destino en cuatro nodos), para la protección de datos en contra de ataques nucleares (la cual solo era para acceso militar, así como para pocas universidades y empresas privadas, quienes la podían utilizar para investigación), se da el inicio de una nueva forma de comunicación digital.

Hacia 1972, introdujo un sistema que facilitaría la comunicación continua denominado Correo Electrónico, para que los usuarios enviaran y recibieran información, aunque se reconoce que en 1971, Ray Tomlinson inventa un programa de correo electrónico para mandar mensajes a través de una red distribuida y manda el primer correo de este tipo, que era un mensaje que decía "Testing 1-2-3" y que iba dirigido a él mismo.

En 1974, se presentó el protocolo "Transmission Control Protocol / Internet Protocol" (TCP/IP), que era un sistema independiente que proporcionaba intercambio de datos entre ordenadores y redes locales de distinto origen, propiciándose un gran desarrollo en las redes administradas por distintos organismos y no de uso exclusivo del la fuerza militar, creándose con esto la red de ordenadores mas grande a nivel mundial: *Internet.*

Internet es la unión de miles de redes informáticas conectadas entre sí, mediante una serie de protocolos (TCP/IP), que hacen posible, para cualquier usuario de una de estas redes, comunicarse o utilizar los servicios de cualquiera de las otras.

Su aplicación más conocida, pública y multimedial es la *World Wide Web (WWW)* ó *Web*[13], que consiste en la mensajería electrónica de textos libres ó archivos planos, que permite la transmisión de datos, imágenes, gráficos, videos, documentos y sonidos a través de un lenguaje común de Hipertexto (HTML Hypertext Markup Language).

Para que podamos visualizar todo tipo de información por la *Web,* se requiere de Browsers, que son navegadores que nos permiten viajar en internet, teniendo entre otros a Netscape Navigator e Internet Explorer, (este último creado por Microsoft).

Como lo mencionamos en el Capítulo Primero, uno de los servicios básicos más utilizados en internet, es el correo electrónico o también denominado *e-mail*, el cual consiste en el intercambio de correspondencia vía electrónica y que permite la comunicación de persona a persona.

El correo electrónico representa todos los sistemas y mecanismos por los cuales el mensaje entra hacia el interior de una conexión de red y su dispositivo encuentra su camino al dispositivo destinatario.[14]

Tenemos que para que esta comunicación se propicie, los usuarios deberán registrarse con algún proveedor de servicio de Internet (ISP), por ejemplo Prodigy y contar con una dirección electrónica, la cual cuenta con los siguientes elementos:

Identidad de inicio de sesión,
Identidad de su ISP,
Ambas separadas por el símbolo @[15](arroba),
Seguido del nombre de dominio (DNS Domain Name System), el cual es una secuencia de etiquetas separadas por puntos y que permite localizar e identificar fácil un sitio de internet,

[13] Creada por Tim Berners-Lee en 1990.
[14] Loshin, Pete. Essential Email Standards: RFCs and Protocols Made Practical. USA, Wiley, 2000. p. 5.
[15] El uso de la @ para el correo electrónico fue un invento de Ray Tomlinson. El significado que se da en lengua anglosajona a la arroba informática es "at", es decir, "en".

traducir nombres a números y permite a los usuarios recordar o familiarizarse con palabras y no con números las direcciones de IP (Internet Protocol).

Los nombres de dominio se utilizan para personalizar la dirección de correo electrónico y para localizar sitios de Internet.

Existen varios tipos de Top Level Domain (TLD):

Genéricos (GTLDS Generic Top Level Domain):

.com (Sitio *web* referente a lo comercial), .net (a la red), .org (Entidad sin ánimo de lucro), .aero (para el ámbito de la aviación), .mil (militar), .edu (educación), entre otros

Códigos de país (CCTLD Country Code Top Level Domain)

.mx (México), .fr (Francia), .au (Australia), .es (España), .br (Brasil), entre otros.

Y tenemos que dentro de cada GTLDS, como por ejemplo dentro de los comerciales podemos encontrar: .tv (televisión), .tm* (marca registrada), .un (pornografía), entre otros.[16]

Por lo que una dirección de correo electrónico, por ejemplo se formaría de la siguiente manera:

sonialazcano@hotmail.com

Y una dirección de un sitio de Internet podría ser:

www.ford.com.mx

[16] "Qué es el sistema de nombres de dominio de internet" s/f, http://gac.icann.org/web/about/gac-outreach_Spanish.htm (Oct.16, 2005)

Aunado al crecimiento de internet, paralelamente se va desarrollando y facilitando el uso del correo electrónico, y que este ha diferencia del correo tradicional, cuenta con los siguientes beneficios:

1.- Facilita la comunicación entre personas, de cualquier parte del mundo.
2.- Rapidez, en virtud de que esta comunicación puede realizarse en forma instantánea dependiendo del tamaño del mensaje que se desee enviar.
3.- Costo, el envío de mensajes no tiene costo alguno, salvo que el usuario desee incrementar la capacidad de almacenamiento, el proveedor del servicio le cobrara una cantidad por el mismo.

Además de facilitar la comunicación entre personas, el correo electrónico es una herramienta para el comercio electrónico, ya que a través de este, las empresas reducen las barreras tradicionales de entrada a los mercados, disminuye costos, distancias e infraestructura, hay mejoras en la distribución, atención a clientes y proveedores: soporte, desarrollo de relaciones, retención y atracción de nuevos clientes y propicia la competitividad de las empresas a escala internacional. En cuanto a los clientes, les facilita la investigación, comparación de mercados y el acceso a más información.

El correo electrónico a través de Internet constituye un medio propicio para la oferta de una gran variedad de productos y servicios, entre los que se destacan los financieros, turísticos y de entretenimiento. Teniendo entonces, que la mayoría de las empresas utilizan el correo electrónico, para informar a los clientes acerca de sus diferentes productos y servicios, y mantienen una relación constante con el cliente a través de su publicidad, y esta gracias al lenguaje multimedia (Introducción de imágenes, sonidos, textos y otras fuentes creativas), ha utilizado el recurso del correo electrónico como un espacio publicitario de gran interés.

El interesado al abrir su cuenta de correo electrónico, puede observar que ha recibido una serie correos publicitarios a través de los cuales, puede conocer un producto y servicio en

cuanto a su calidad, precio y demás condiciones; también denominadas comunicaciones comerciales, que la Directiva 2000/31/CE en su Art. 2 f), las define como: "Toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional".

En Internet tenemos dos tipos de estrategias de publicidad el "*push*" y el "*pull*": "Cuando la estrategia es de *push*, la empresa / marca empuja el producto a través de la distribución hacia el consumidor, engrasando el camino mediante técnicas de ventas, márgenes, condiciones y promociones a los intermediarios, y en la confianza de que cada uno de éstos se esfuerce por llevar al producto al siguiente eslabón con preferencia sobre los productos competidores. Cuando la estrategia opta por *pull*, el símil es de lanzar la marca un cable con un gancho hacia el consumidor y, una vez enganchado a éste, tirar de la cuerda para acercarlo al punto de venta. Las dos estrategias suelen ser complementarias"[17], podríamos mencionar entre otros a los Banners[18] como *pull*.

Estas estrategias han facilitado el envío de mensajes a gran escala, teniendo que no siempre los usuarios desean recibir publicidad, y que estos reciben mensajes que no han solicitado o inclusive mensajes provenientes de empresas u organizaciones que no conocen, o que no saben su procedencia, dando pauta a que el correo electrónico se utilice como canal de difusión publicitaria sin el consentimiento del usuario, facilitándose así el envío de *mensajes no solicitados*.

[17] Barnes Vázquez, J. Internet y el *Derecho.Una nota acerca acerca de la libertad de expresión e información en el espacio cibernético* 1ª. Ed. Madrid, Ordenación de las Telecomunicaciones, 1997. p. 237

[18] Gráfico publicitario rectangular que puede ser fijo o animado, e incluso con sonido, que se incluye en las páginas web a modo de anuncio. Haciendo click sobre él, normalmente envía hacia el sitio web del anunciante. "Definición de banner" s/f, http://www.definicion.org/banner (Oct. 18, 2005)

2. Correo Electrónico No Deseado

Como lo puntualizamos en el apartado anterior, los usuarios de Internet a través de su cuenta de correo reciben correspondencia proveniente de remitentes desconocidos, esto se puede dar a través de virus informáticos de la red, o porque obtuvieron sus datos personales como lo es su dirección correo electrónico, entre otras causas.

El contenido de estos mensajes electrónicos puede ser variado: ya sea para visitar algún sitio de Internet, publicitarios, para ofertar productos o servicios para que sean adquiridos por medio del e-mail, cadenas (que son mensajes masivos que se envían a decenas de personas y que al reenviarlos se multiplican hasta por miles o millones de mensajes), o bien estos pueden tener contenidos que dañen moralmente al usuario. Teniendo que estos mensajes, resultan molestos para el usuario ya que en ocasiones llenan la capacidad de su cuenta que le fue otorgada por el proveedor de servicios de Internet, así como perder el tiempo del usuario para eliminarlos.

A este tipo de mensajes se les conoce como *correo basura, correo no deseado, correo no consentido, Spam, Junk e-mail* ó *Unsolicited Bulk e-mail.*

2.1 Origen

"Spam" es el acrónimo de "Spice Ham", que se refiere a un tipo de carne de cerdo enlatada comercializada por Hormel Foods Corporation surge en los años 20, y se hizo famosa porque se utilizó durante la Segunda Guerra Mundial para alimentar a las tropas norteamericanas.

La utilización del término *Spam* asociado a productos "no deseados" se atribuye a cierto capítulo de la comedia "Monty Phyton's Flying Circus" en 1970, en el cual la escena se desarrolla en un restaurante al que van a comer un hombre y su esposa, en el cual sirven

spam en todas sus comidas. Los clientes se ven obligados a comer *spam* y no existe forma de pedir un plato que no lo contenga. Durante el desarrollo de la escena hay cantos de unos vikingos (que ocupan la mesa contigua), en que se repite el término "*spam*, *spam*, *spam*" hasta sofocar toda otra comunicación, por lo que en este sentido se le denomina así al correo electrónico no deseado.

El 3 de mayo de 1978, es el primer reporte que se tiene del *Spam*, cuando un empleado de Digital Equipment utilizó el directorio de correos del entonces ARPANET, para anunciar la nueva serie de servidores DEC-20. Desde entonces, la complejidad y métodos utilizados para el envío de correspondencia no deseada, ha evolucionado hasta transformarse en una situación que afecta a la mayor parte de los usuarios de correos electrónicos.

Se afirma que a partir de 1994, el *Spam* se vuelve una práctica comercial que utiliza métodos irregulares y que representa una gran problemática en el entorno de la red, mencionando que en esa época uno de los casos más famosos fue el de "Green Card Lottery – Final One?", para promocionar servicios de inmigración, y que a partir de ese tiempo, surge una gran variedad de formas y tipos de *Spam*.

2.2 Definición

Tener una definición del término *Spam*, resulta complicado, ya que en virtud de su origen es un término que se utiliza como algo no deseado, y no existe aún una definición a nivel internacional de este fenómeno, por lo que en este trabajo lo definiremos como:

Todo correo electrónico no solicitado, no deseado o no consentido, y que es transmitido a un número importante de direcciones, con o sin el consentimiento del usuario.

En la Web, podemos encontrar múltiples definiciones del correo basura, entre otras tenemos:

Se llama *Spam* a la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados. Generalmente, se trata de publicidad de productos, servicios o de páginas Web.[19]

La palabra "*Spam*" aplicada al e-mail significa Correo Electrónico Masivo No Solicitado (*Unsolicited Bulk Email "UBE"*). No solicitado significa que el receptor no dio un permiso verificable para que se le envíe el mensaje y masivo significa que el mensaje es enviado como parte de una colección mayor de mensajes, donde todos tienen el contenido sustancialmente idéntico.[20]

2.3 Características

En tanto no exista un concepto lingüístico del *spam*, ni consenso internacional para definirlo, podemos mencionar sus características, entre las cuales tenemos:[21]

- Correo electrónico no deseado, no solicitado.
- Correo basura que proviene de terceros.
- Usualmente de naturaleza comercial.
- Envío masivo, repetitivo.
- El receptor nunca ha tenido contacto previo con el emisor.

2.4 Clases de *Spam*

Asimismo encontramos diversas clases de correo basura *Spam* enviado a través del correo electrónico.

- *Spim*: específico para aplicaciones de tipo Mensajería Instantánea (MSN Messenger, Yahoo Messenger, etc).

[19] Siccardi, Eugenio. "Spam" s/f. http://www.rompecadenas.com.ar/spam.htm (Oct. 20, 2005)

[20] "Definición de Spam" s/f. http://www.spamhaus.org (Oct. 20, 2005)

[21] "Qué es el Spam" s/f. http://www.profeco.gob.mx (Oct. 18, 2005)

- *Spit*: *spam* sobre telefonía IP. La telefonía IP consiste en la utilización de Internet como medio de transmisión para realizar llamadas telefónicas.
- *Spam SMS*: *spam* destinado a enviarse a dispositivos móviles mediante SMS (Short Message Service).

Y muy recientemente:

- *Splogs:* que sirven para promocionar desde páginas de web juegos de azar hasta pornografía, a través de las bitácoras por Internet conocidas como Blogs.

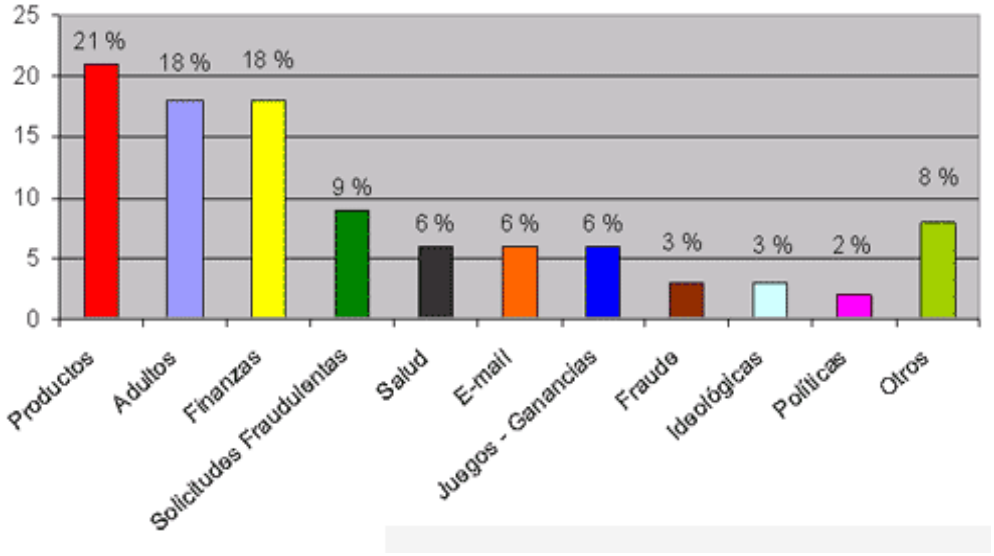
De los anteriormente mencionados el más común, es el correo electrónico *Spam.*

2.5 Ejemplos más comunes de *Spam*

En la actualidad, encontramos una gama de *spams*, sin embargo, tenemos entre los *Spams* más populares:

1. Venta de medicinas milagrosas para enfermedades como el cáncer, SIDA, diabetes, entre otros.
2. Medicamentos para adultos como el valium, viagra de los más comunes.
3. Productos para bajar de peso en forma rápida y efectiva
4. Phishing (es un correo electrónico falso que solicita información financiera).
5. Premios como la lotería.
6. Joyería (relojes).
7. Gente desaparecida.
8. Fraude nigeriano (Carta nigeriana).
9. Oportunidades de negocio o de inversión.
10. Ofertas de trabajo.
11. Servicios financieros (Ahorro, créditos, préstamos).
12. Computadoras, software, hardware.
13. Pornografía.
14. Productos varios (Libros, música y juegos).

15. Paquetes vacacionales.
16. Casinos.
17. Esquemas piramidales, para hacerse de una gran fortuna.
18. Venta de títulos y de grados académicos.
19. Políticos o ideológicos.
20. Religiosos.



[22].

Los *Spams* por lo general llegan al usuario en forma de cadena, con faltas de ortografía, con comandos que desconocemos, fotografías y de imágenes que llaman y captan su atención, y al dar respuesta a este tipo de correo, se verifica que la cuenta de correo en

[22] "Clasificación del SPAM, según contenido o productos comercializado" s/f. http://www.pc-news.com (Oct.16, 2005)

donde se recibió el mensaje es válido y con esto a reproducir más *Spam*. A manera de ejemplificar un *Spam*, los podemos encontrar como se muestra a continuación[23].

--- Mensaje original ---

Subject: RV: RV: NIÑO DESAPARECIDO HIJO DE UNA COMPAÑERA DE SCH!!!!

Por favor mira la foto y reenvíala.
Por favor les ruego a todos los que conocen este e_mail, o no, que envíen este correo al mayor número de personas conocidas posible.
Tengo un hijo de 5 años de edad que está perdido desde el 11 de mayo del 2002.
Si alguien, en cualquier lugar, sabe algo o lo ha visto, porfavor comuníquese con
MERCEDES ARROYO FLORES
Dpto. de Instalaciones y Mto Std
SEGURIDAD Y MANTENIMIENTO, S.A. (BANCO SANTANDER CENTRALHISPANO)
TLFNO: 91 774 95 41 Fax:91 468 62 11
E-MAIL: MERARRO@SEGURCONTROL.COM

Todas las oraciones serán agradecidas!!!
Sólo tardará 2 segundo en enviarla, si este fuera tu hijo toda desearías la ayuda del mundo que te pudieran prestar.

Gracias de corazón.

La simple conexión a una dirección, implica que el programa de navegación le transmite la siguiente información a dicha web: la dirección TCP/IP, la marca y versión del programa

[23] "Niño desaparecido" s/f. http://www.vsantivirus.com/hoax.htm (Oct. 18, 2005). Otros ejemplos de *Spam* Ver Anexo 1

de navegación, la marca y versión del sistema operativo, lengua que maneja el usuario, pagina de referencia y las cookies[24] eventuales ya enviadas, las cuales pueden proporcionar información de elementos que afectan la identidad económica, cultural o social de un usuario como lo es su nombre, domicilio, estado civil, profesión, escolaridad, empresa para la cual trabaja, estados de cuenta, religión, preferencias sexuales, por mencionar algunas.

El correo no solicitado es un medio que facilita el envío de virus, spywares, (Sistemas que espían y roban la identidad y datos[25]), provoca la pérdida o alteración de datos de los usuarios, así como el poder realizar conductas ilícitas de personas malintencionadas (que abundan en la red), como es el fraude (Scam), piratería, pornografía infantil, Sniffing, Phishing y Pharming[26]. Afecta también a las comunicaciones, ya que al saturarse la casilla o bandeja de correo del usuario, este no podrá recibir correos que desee o que sean de su interés, hasta que no sean eliminados, ocasionándole pérdida de tiempo a la entrada a su bandeja como al borrarlo, propiciando el colapso en la cuenta de correo y en la línea de acceso a la red, así como la saturación de las redes, lentitud del sistema de Internet junto con enormes pérdidas económicas y de productividad tanto para las empresas como para el propio usuario.

Teniendo entonces, que los usuarios se encuentran vulnerables ya que es a través de este medio por el cual, cualquiera puede tener sus datos personales sin que lo sepan, por lo que este problema trae consigo el daño hacia la privacidad y confidencialidad de información de los usuarios en la red y por ende la desconfianza en la Web.

[24] Se crean con la intención de convertirse en un espía virtual que alerte a las direcciones *Webs* que las introducen sobre los datos y preferencias de sus visitantes

[25] Como son los programas de intercambio de archivos, entre los más populares podemos mencionar a Kazaa, eDonkey o eMule.

[26] Sniffing, Phishing y Pharming, normalmente se usan con fines ilegales para el robo de información.

3. Protección de Datos Personales

No hay duda de la importancia que las tecnologías de la información y de la comunicación han alcanzado en los últimos años. Las llamadas TIC (Tecnologías de la Información y de la Comunicación) han entrado a nuestra sociedad de un modo extremadamente acelerado, produciendo una auténtica revolución de la información, del mismo modo que en su día fue la revolución industrial; amenazando con transformar por completo nuestra idea de sociedad y de las estructuras que la conforman.

Por lo que es importante mencionar el régimen jurídico inherente a México y a algunos países sobre la protección al Derecho a la Información.

En nuestra Carta Magna, tenemos en el capítulo de Garantías Individuales las disposiciones que hacen referencia a la libertad de expresión, al derecho a estar informados, a los límites de los medios para manifestar ideas, principio de legalidad e inviolabilidad de la correspondencia:

El derecho a la información, consignado en el artículo 6 constitucional, es un derecho subjetivo público cuyo titular es todo gobernado, independiente de que también sea de índole social, estableciendo que:

Art. 6: “La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito o perturbe el orden público; el derecho a la información será garantizado por el Estado”.

Este derecho garantizado por el Estado, corresponde a la obligación correlativa de rendir la información que se solicita para acceder y examinar datos y registros públicos por parte de los gobernados (Habeas Data). Esta obligación por ser de carácter público como todas las

concernientes a cualquier derecho del gobernado reconocido y plasmado en la Constitución, incumbe a todo órgano estatal, pues sin ella sería meramente utópico por no decir inexistente, teniendo a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el Diario Oficial de la Federación el 11 de Junio de 2002, que apoya el precepto constitucional mencionado y es a través del Instituto Federal de Acceso a la Información Pública que lo realiza.

Pero este acceso a la información, se ve limitado en materias como la electoral, reservas petroleras, entre otras, justificando el Estado que por causas de seguridad nacional no proporciona dicha información.

El Art. 7 señala: "Es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública…".

Aunque solo determina el medio impreso, este artículo se aplica en cuanto a los limitantes que no dañen a la vida privada, moral y a la paz pública en cualquier medio de difusión como lo es internet.

Mientras que el Art. 16 establece que: "Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud del mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento…".

Es decir, no puede violarse la intimidad de ninguna persona sin mandamiento judicial escrito, fundado y motivado para ser molestado en su persona, familia, domicilio, papeles o posesiones.

Y en su párrafo décimo segundo señala que: "… La correspondencia que bajo cubierta circule por las estafetas, estará libre de todo registro, y su violación será penada por la

ley…", por lo que se prohíbe la violabilidad de la correspondencia, y que en nuestra opinión en este párrafo debería incluir lo relativo a la correspondencia electrónica.

Teniendo entonces, que se contraponen tanto el derecho a la libertad de expresión y el derecho a la intimidad, en nuestra opinión es recomendable que en una norma jurídica se precise: 1) la vía previa que pueden acudir los ciudadanos en caso que viesen vulnerados sus derechos de intimidad, acceso de información de entidades públicas (Hábeas Data) honor, buena reputación, rectificación de información inexacta y 2) La calificación expresa de los datos públicos, así como de datos privados para su resguardo.

En el Derecho comparado, las primeras normas sobre esta materia se remontan a la década de los 70. En los Estados Unidos de Norteamérica se dicta la Privacy Act en 1974, buscando salvaguardar la privacidad personal (detonador del sistema jurídico de ese país en esta materia), en tanto derecho individual puesto en jaque por las grandes recopilaciones de datos públicos y privados que comenzaban a predominar en la época gracias al poder de memoria y cálculo de las grandes máquinas.

En Europa se vive un proceso similar a partir de las leyes conocidas como "de primera generación", que comienzan en Alemania con el Land de Hesse (1970), y Datalag o Ley de Datos en Suecia (1973), pero que continúan en años sucesivos hasta abarcar prácticamente la totalidad de los estados miembros de la Comunidad. Estas primeras leyes, junto con la francesa de 1978 (Nº 78-17), que entre otras disposiciones crea la Comisión Nacional de Informática y Libertades, eran muy reglamentaristas y limitacionistas al encuentro de los tratamientos automatizados con los datos nominativos. En particular prevén y regulan minuciosamente el registro de las bases de datos que contengan datos de esta naturaleza, con pocas exclusiones.

En cambio las denominadas "leyes de segunda generación" se inspiran en el modelo alemán de autorregulación (1984), que da cuenta de la extensión de la microinformática en la trama social, y con ello la multiplicación enorme de este tipo de ficheros, de todo tamaño

y no necesariamente radicada en unos pocos y privilegiados lugares. En esta segunda ola normativa se permite, pues, el procesamiento de este tipo de datos tanto cuando el particular ha dado su consentimiento, como cuando el derecho lo permite en virtud de ciertas razones todas ellas muy razonables, puntuales y apriorísticas que las propias normas se encargan de enumerar, teniendo en esta generación a la ley española Ley Orgánica 5/1992 de 29 de octubre de 1992 conocida como L.O.R.T.A.D: Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal.

En algunos países, el fenómeno de la informatización de la sociedad y sus repercusiones sobre los derechos de las personas llega a ser considerado de tal magnitud que se dictan normas de protección constitucional. Así Portugal (1976) y España (1978). En América Latina son los casos mucho más recientes del Brasil (1988), Paraguay (1992), Perú (1993) y Argentina (1994).

La normativa supranacional europea es, quizás, el modelo mejor logrado de regulación en esta materia, ya que en ella encuentran desarrollo la mayor cantidad de aspectos expresivos del régimen, incluyendo la cuestión propiamente internacional (flujos de datos transfronterizos, que el Consejo Económico de la Organización de las Naciones Unidas lo define como la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y recuperación).

Se trata, fundamentalmente, del Convenio 108 del 28 de enero de 1981 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales, norma que resulta ampliada y actualizada por la Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

4. Propiedad Intelectual de la Información

La electrónica ha hecho posible el almacenamiento y utilización de tal cantidad de datos que antes sólo existían en ficheros privados, y que puede violar la intimidad de las personas por medios y sistemas que no estaban al alcance de nuestros inmediatos antepasados. Ante este fenómeno, es necesario considerar en qué forma la ciencia jurídica puede realizar la protección de datos y el derecho a la intimidad.

Por protección de datos, se entiende a la protección jurídica de las personas en lo que concierne al tratamiento de sus datos de carácter personal, o expresado de otra forma, el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional en los límites de su intimidad.[27]

El bien jurídicamente protegido inherente a la protección de datos es la privacidad o intimidad que se entiende como el derecho del individuo a decidir por sí mismo en que medida quiere compartir con otros su pensamiento y sentimientos, así como los hechos de su vida personal.

La información que afecta la intimidad personal y familiar podemos decir, es la que contiene los siguientes datos cuando son divulgados sin autorización o consentimiento de la persona o sin orden judicial o de la autoridad competente expresa:

a) Datos sensibles, como son el de raza, ideología, estado de salud, creencias, religión.

b) Datos secretos, como son el secreto profesional, secreto bancario, etc.

[27] Davara Rodríguez, Miguel Ángel. *La Protección de Datos en Europa.* Madrid, Universidad Pontificia Comillas ICAI-ICADE, 1998. p. 9

c) Datos reservados, siendo aquellos que el titular no está obligado a proporcionar para que sean conocidos por terceros, como son: filiación (hijo de matrimonio, extramatrimonial, adoptado), delitos contra el honor (difamación, calumnia, injuria), libertad sexual (violación), adulterio, aborto, etc.

d) Datos privados, los que el titular debe proporcionar periódicamente a la autoridad para fines específicamente señalados, como por ejemplo los datos contenidos en una declaración del impuesto sobre la renta, y que sólo deben ser utilizados para los fines que específicamente fueron dados, no para fines distintos.

En la Declaración Universal de los Derechos Humanos establece en su Art. 12, el derecho a la intimidad, señalando: “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación”.

La Convención Europea para la protección de personas sobre el tratamiento automatizado de datos de carácter personal, firmado en Estrasburgo en 1981, establece en su Artículo 1, que su objetivo es garantizar sobre el territorio de cada parte, a toda persona física, cualquiera que sea su nacionalidad o su residencia, el respeto de sus derechos y de sus libertades fundamentales, en particular el derecho a su vida privada, en relación con el tratamiento automatizado de la información de carácter personal.

En México no existe aún una ley en cuanto a la protección a los datos personales, ya que únicamente en materia de propiedad intelectual (que es el conjunto de derechos patrimoniales de carácter exclusivo que otorga el Estado por un tiempo determinado, a las personas físicas o morales que llevan a cabo la realización de creaciones artísticas o que realizan invenciones o innovaciones y de quienes adoptan indicaciones comerciales, pudiendo ser estos, productos y creaciones objetos de comercio), se protege en la Ley Federal del Derecho de Autor a los sistemas de cómputo y bases de datos, y en particular en cuanto a estos últimos tenemos que:

Art. 107: “Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos”.

Art. 108: “Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años”.

Art. 109: “ El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.
Quedan exceptuados de lo anterior, las investigaciones de las autoridades encargadas de la procuración e impartición de justicia, de acuerdo con la legislación respectiva, así como el acceso a archivos públicos por las personas autorizadas por la ley, siempre que la consulta sea realizada conforme a los procedimientos respectivos”.

Asimismo, tenemos en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[28], en su Art. 3 frac. II, la definición de Datos Personales como: “La información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad”. Y tiene en su Capítulo IV referente a la protección de datos personales.

Artículo 20: “Los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:

[28] “Datos personales” s/f. http://www.ifai.org.mx/datos_personales/nacionales.htm (Oct.20, 2005)

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;
II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;
III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;
IV. Procurar que los datos personales sean exactos y actualizados;
V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y
VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado".

Artículo 21: "Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información".

Artículo 22: "No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:
I. (Se deroga).
II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
IV. Cuando exista una orden judicial;
V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y
VI. En los demás casos que establezcan las leyes".

Artículo 23: "Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales".

Artículo 24: "Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.
La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27".

Artículo 25: "Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales.

Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones".

Artículo 26: "Contra la negativa de entregar o corregir datos personales, procederá la interposición del recurso a que se refiere el Artículo 50. También procederá en el caso de falta de respuesta en los plazos a que se refieren los artículos 24 y 25"[29].

Asimismo, existe ya la iniciativa de ley sobre la protección de datos personales y actualmente es materia de estudio en la Cámara de Diputados, por lo que en virtud de la falta de protección que se tiene en lo que hace a la información privada, sería importante que se agilizara la discusión como la aprobación en esta Cámara.

Por lo que aun queda mucho por hacer en materia de apropiación de la información y protección a datos personales en nuestro país.

En el panorama Internacional tenemos que la Organización Mundial de la Propiedad Intelectual (OMPI), mantiene un papel proactivo en cuanto a la elaboración de normas para la protección de la propiedad intelectual y en específico sobre las bases de datos, dicho organismo organizó una reunión de información sobre la propiedad intelectual en materia de bases de datos en Ginebra que hacía énfasis a la posibilidad de brindar una protección sui generis a las bases de datos.

Teniendo en el Tratado de la OMPI sobre Derechos de Autor, así como en el Acuerdo sobre los Aspectos de los Derechos de la Propiedad Intelectual Relacionados con el

[29] "Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental" s/f. http://www.ifai.org.mx/transparencia/LFTAIPG.pdf (Oct. 20, 2005)

Comercio (ADPIC) y en el Tratado de Libre Comercio de América del Norte (TLCAN) entre otros, la protección sobre compilaciones de datos.

5. Impacto económico del *Spam*

Considerando los puntos anteriores, el *spam* no sólo daña la privacidad de los usuarios y es un medio por el cual se pueden cometer delitos, tenemos que los resultados en el crecimiento de esta práctica ilícita, ha traído consigo el impacto económico en el comercio electrónico ocasionando grandes pérdidas a las empresas, organizaciones y a los particulares.

De acuerdo a la nota periodística de Lilia Chacon, publicada en el Periódico Reforma, el 5 de Septiembre de 2005, "Durante el pasado mes de julio, el 72 por ciento de los correos electrónicos que se enviaron a nivel mundial fueron correos basura (*spam*), lo que representa un crecimiento de 15 por ciento más, frente al mes inmediato anterior, según el informe de la empresa IronPort Sistems…"[30]

Así mismo señala que "el principal proveedor es Estados Unidos, con cerca de 52 mil millones de mensajes al mes, seguido por China, Corea del Sur, Brasil, Gran Bretaña, Japón, Francia, Canadá, Alemania y España, quien a México en el top de los 10 países como principales generadores de *spam* en el mundo". Y señala que "Por contenido, el estudio semestral de Sophos describe los 5 principales tópicos de estos mensajes son con publicidad y venta de medicamentos con 41.4 por ciento, préstamos hipotecarios con 11 por ciento, 9.5 por ciento es contenido para adultos, 8.5 por ciento son estafas y 8.3 con la venta de productos en general". Especificando que en julio, México se generó 2,615 millones de correos basura…".

[30] "Ocupa *spam* 72% en correo mundial" s/f. http://www.reforma.com/Negocios (Oct. 20, 2005)

El crecimiento tan vertiginoso del S*pam*, trae daños económicos incalculables que mes por mes reportan las empresas y que en el caso concreto de México y de acuerdo al periódico nacional La Jornada los correos basura ocasionan pérdidas por $6.5 millones de pesos al mes, como lo señala la nota periodística de Víctor Cardoso publicada el 24 de marzo de 2005, cuya parte medular transcribo a continuación:

“Circulan mil 460 millones de esos mensajes diarios en el país, informan especialistas

En México los correos basura ocasionan pérdidas por $6.5 millones al mes
El problema daña la calidad de los servicios y satura las telecomunicaciones

A pesar de las dimensiones y las pérdidas económicas que genera el correo electrónico basura *(spam)* en el mundo, todavía se carece de información y de legislaciones adecuadas para su combate que, en principio, requiere acciones globales para evitar que continúe dañando la infraestructura, los servicios y el desarrollo de las comunicaciones electrónicas.
Esas fueron las conclusiones a que llegaron investigadores y funcionarios de México y Estados Unidos que participaron en el foro *El spam y su impacto*, organizado por la Universidad La Salle, en coordinación con la Comisión Federal de Telecomunicaciones (Cofetel).
A pesar de la falta de información sobre los efectos, el director de la empresa de telecomunicaciones NIC de México, Oscar Robles Garay, dijo que en el país se supone la transmisión de por lo menos mil 460 millones de correos electrónicos no solicitados, lo que representa pérdidas económicas por 6.5 millones de pesos al mes.
La subdirectora de Instrumentación Legal de la Cofetel, Claudia Fonseca Martínez, dijo que algunas otras cifras permiten considerar que tres cuartas partes (75 por ciento) del correo electrónico mundial es *spam*; de ese porcentaje, 63 por ciento se produce en Estados Unidos; 21 por ciento en la región Asia Pacífico; 13 por ciento en Europa, y 3 por ciento en América del Sur.
Afirmó que además de generar daños en la productividad y competitividad de las empresas, el *spam* afecta a la infraestructura informática al propiciar el uso inútil de banda ancha, la

denegación del servicio por saturación y la transmisión de virus y *gusanos*, lo que provoca servicios de telecomunicaciones menos eficientes, a costos elevados.
El *spam*, precisó, se distingue porque es un correo no solicitado, comercial o de contenido ilícito, de distribución masiva y emisor desconocido, que evoluciona con la tecnología y que en algunos casos es involuntario pues se distribuye a partir de un virus informático. No obstante, justificó su existencia por el hecho que es un negocio que genera publicidad y beneficios económicos casi sin costo para quienes lo envían…"[31].

Es importante señalar, que esta práctica importa beneficios a unos cuantos, como lo son los Spammers, quienes obtienen un lucro al recolectar datos para su posterior venta (inclusive son contratados por empresas), y generan publicidad y beneficios económicos casi sin costo y que de acuerdo al reporte de resultados de la reunión celebrada en Busan Corea, Task Force on Spam OECD, de septiembre de 2004, la ganancia diaria aproximada de estos, oscila entre los 8,000 dólares por día.

El envío masivo de estos correos, no tan solo propicia pérdidas económicas para las empresas, si no también para los usuarios de carácter particular, ya que ocasiona que los servicios de las Telecomunicaciones sean menos eficientes y provoca que se eleven los costos del servicio y estos son asumidos por los particulares al estar más tiempo en Internet o bien provocando la interrupción continua del servidor de Internet, obligándolo a conectarse en más ocasiones. Como se puede observar, la falta de disposiciones legales ante este creciente problema en materia del *spam*, ocasiona graves problemas económicos y desde mi particular opinión a frenado el desarrollo del comercio electrónico, en virtud de todos los daños que ocasiona esta práctica nociva.

[31]"Circulan mil 460 millones de esos mensajes diarios en el país, informan especialistas s/f. http://www.jornada.unam.mx/2005/03/24/019n1eco.php (Oct. 21, 2005)

Capítulo III Regulación Jurídica Internacional del *Spam*

1. Estados Unidos de América

En virtud de que Estados Unidos de América, es el país que más produce *Spam* en el mundo, ha llevado a cabo una ardua tarea para legislar esta problemática, teniendo como primera Ley de carácter Federal la CAN-SPAM ACT[32], que es vigente a partir del primero de enero de 2004, misma que regula las comunicaciones comerciales electrónicas emitidas por correo electrónico, con el objeto de controlar su práctica. Esta ley permite asignar daños de hasta dos millones de dólares americanos a los infractores de la ley, enviar a los spammers a la cárcel (hasta 5 años), o bien a pagar hasta el triple del valor de los daños si se determina que la violación fue intencional o que posee encabezados falsos (considerándolo como un crimen menor).

La CAN-SPAM ACT, consiste básicamente en un sistema *opt-out,* que permite el envío del correo electrónico comercial, hasta en tanto el destinatario solicite que no se le envíe más, es decir, la CAN-SPAM ACT no prohíbe los correos no deseados, sino que autoriza a los usuarios de Internet a reclamar su salida de las listas de difusión y castiga a los que envían mensajes engañosos o con carácter pornográfico sin advertir previamente a los que lo reciben.

Esta ley señala que las empresas o los que se dediquen al mercadeo pueden enviar estos correos, siempre y cuando:

- Marquen claramente los mensajes que son publicidad.
- Usen una línea de asunto relevante al contenido.
- Usar direcciones de correo válidas del remitente.
- Proveer una dirección física valida.

[32] "CAN SPAM Act" s/f. http://www.spamlaws.com/federal/can-spam.shtml (Oct.18, 2005)

- Proveer una opción que le permita al público cancelar o detener el envío de publicidades futuras.
- Procesar solicitudes de bajas en los siguientes diez días hábiles.

Esta opción obliga a los emisores a satisfacer el deseo de aquellos receptores que manifiesten su voluntad en el sentido de no recibir más correos de tal tipo.

El Acta de CAN-SPAM le da a la Comisión Federal de Comercio (Federal Trade Commission, FTC), la autoridad de hacer cumplir las condiciones y de establecer sanciones por violaciones, así como, ser la autoridad competente de supervisar (Enforcement), a esta clase de correos, con el objeto primordial de la defensa del consumidor, también le da a los procuradores generales de los estados, autoridad limitada para hacer cumplir ciertas condiciones del Acta.

Dentro de las funciones de la FTC, es la creación de un registro nacional "Do-Not-E-Mail-Registry", en donde pueden inscribirse los usuarios que no desearan recibir mensajes publicitarios. También cuenta con el buzón de *Spam* en donde los usuarios pueden reenviar a él los correos electrónicos que reciban y que ellos mismos consideren *Spam*[33]. Y cuenta con una base de datos que hace las veces de un guardián del consumidor (Consumer Sentinel), en donde se reciben quejas de los usuarios.

Teniendo que los más grandes proveedores de servicios de Internet (ISP) americanos, AOL (grupo Times Warner), Microsoft, Yahoo y Earthlink, ya llevan a cabo sus ofensivas judiciales en contra de los emisores de S*pam*, a partir de la entrada de esta ley, como fue el caso que interpuso en diciembre de 2003, la empresa Microsoft (propiedad de Bill Gates), en contra de Scott Richter conocido o nombrado como "Rey del Spam".

[33] La dirección del buzón es: uce@ftc.gov.

En el cual, la fiscalía de Nueva York, impuso en agosto de este año, una sanción económica de siete millones de dólares por todos los daños causados por los envíos masivos de correos no solicitados a la empresa OptInRealBig.com, propiedad de Scott Richter, comprometiéndose este a no enviar más *Spam,* salvo para aquellos usuarios que le autoricen su envío, sin embargo las autoridades ordenaron su salida del registro de Spammers y continuarán vigilándolo para que ya no realice más esta práctica.

Microsoft informó, que destinará cinco de los siete millones de dólares a trabajar con la policía y gobiernos de todo el mundo para purgar la red de todos los peligros de seguridad que la amenazan. Asimismo, donará un millón de dólares en la promoción de centros para niños de bajos recursos de Nueva York[34].

Sin embargo este Spammer no es el único, tenemos a miles de personas que llevan a cabo ese envío masivo en todo el mundo[35].

Es importante mencionar que estos proveedores entre otros, han creado filtros o sistemas de administración de *Spam* y medidas autoregulatorias entre los ISPs, sin embargo, las personas que envían estos correos no deseados buscan o inventan nuevas formas de evadirlos para lograr su cometido.

A pesar de la promulgación de la CAN-SPAM ACT, varios expertos la determinan como muy flexible, ya que a pesar de sus sanciones y del trabajo de la FTC como de sus medidas de seguridad, esta permite la práctica del *Spam*, situación que no contempla la Ley Estatal de California de 1998[36]: Ley contra el correo basura (*antispam)*, considerada como la más rígida de la nación norteamericana, y que declara como ilegal enviar a los californianos publicidad no solicitada por el correo electrónico, así como el envío de correo

[34] Véase Apéndice único

[35] Véase McWilliams, Brian. *Spam Kings*. USA, O´Reilly, 2004.

[36] "States Laws: California" s/f. http://www.spamlaws.com/state/ca.shtml (Oct. 18. 2005)

no deseado desde ese Estado, y la recolección de direcciones de correo electrónico con el propósito de enviar este tipo de correo, salvo que exista una relación previa clara de negocios con el posible receptor o cuando se haya recibido su autorización expresa.

Sus sanciones van desde un dólar por cada mensaje no solicitado hasta un millón de dólares por cada campaña, y permite a los propios usuarios de Internet afectados a demandar a las empresas responsables de los *Spam*, así como al fiscal del Estado y a las firmas que proporcionan los servicios de internet.

2. Unión Europea

Los países Europeos han adoptado el sistema *opt-in*, implementado especialmente en España, la cual promulgó la Ley Orgánica de Protección de Datos[37] (LOPD), y que en este tema de protección a datos personales cuenta con un gran trabajo legislativo, así también la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico[38] (LSSICE 34/2002 del 11 de julio y modificada en noviembre de 2003), que regula a las comunicaciones comerciales y atribuye a la Agencia Española de Protección de Datos (AEPD), la competencia en materia de supervisión del cumplimiento de las normas relativas a comunicaciones electrónicas no solicitadas (*Spam*), y su participación en el plano internacional en el combate antispam.

La LSSICE establece en su Art.21, la prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes:

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no

[37]"Base de datos de Legislación Ley Orgánica de protección de datos" s/f. http://www.juridicas.com/base_datos/Admin/lo15-1999.html (Oct. 18, 2005)
[38]"Asociación española de comercio electrónico Legislación 34/2002" s/f. http://www.aece.org/legislacion.asp (Oct. 18, 2005)

hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Por lo que en base a esta disposición el sistema *opt-in*, consiste en que no se puede enviar correos electrónicos comerciales si el destinatario del mismo no lo ha solicitado, o no ha dado su consentimiento para ello, es decir su prohibición es de carácter relativo, a comparación de la CAN-SPAM ACT, que si lo permite.

Así también, establece una serie de requisitos a los empresarios:

1. Las comunicaciones comerciales deberán ser claramente identificables.
2. Deberán indicar la persona física o jurídica en nombre de la cual se realizan.
3. Si las comunicaciones comerciales se realizan a través de correo electrónico, incluirán al comienzo del mensaje la palabra "publicidad".
4. En los casos de ofertas promociónales, se exige que las condiciones de acceso y de participación se expresen de forma clara e inequívoca.

Determinando que el envío masivo de comunicaciones comerciales por correo electrónico a destinatarios que no lo hayan solicitado o autorizado, así como al envío de más de tres comunicaciones a un mismo destinatario en el plazo de un año, constituye una falta grave y establece multas de 30.000 euros hasta 150.000 euros y en el caso de que no se

pueda considerar grave por no ser masivo, es decir que sea leve, la sanción será de hasta 30.000 euros (Art. 38 LSSICE).

Esta ley otorga una serie de derechos a los destinatarios de los correos no solicitados:

1. Otorgar su consentimiento y estar informado de la recepción de dichos correos.
2. Revocar en cualquier momento el consentimiento otorgado.
3. Establece que el procedimiento de revocación deberá ser sencillo y gratuito.
4. Deberán prestar información accesible por medios electrónicos sobre dichos procedimientos.

Por lo que podemos determinar, que en España esta prohibido el envío de comunicaciones comerciales no solicitadas *Spam*, pero es lícito si estas se autorizan expresamente o se solicitan, teniendo que países como Inglaterra, Austria, Bélgica, Dinamarca, Irlanda, Canadá, Suiza, Australia e Italia, tienen legislaciones similares a la española.

La Directiva de la Unión Europea 2002/ 58/CE[39], del Parlamento Europeo y del Consejo del 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección a de la intimidad en el sector de las comunicaciones electrónicas, adopto este sistema *opt-in*, es decir, prohíbe tanto la remisión de la publicidad no consentida como aquella a la que se le ha negado la recepción y el envío de correos electrónicos con fines de venta directa si el remitente oculta o disimula su identidad o si no se concreta una dirección válida a la que el destinatario pueda pedir su no envío y la facilitación de mecanismos de oposición a estos.

Reconoce la posibilidad de que los Estados intercepten, de acuerdo con la legalidad, las comunicaciones electrónicas o tomen las medidas necesarias en razón de la protección de la seguridad pública, la defensa, la seguridad del Estado y aplicación del Derecho Penal. Destaca en el Art. 5, la confidencialidad de las comunicaciones y en el Art. 6, prevé la

[39] "Spam Laws, European Union/EEA" s/f. http://www.spamlaws.com/eu.shtml (Oct. 20, 2005)

eliminación o la conversión en anónimos de los datos de tráfico cuando dejen de ser necesarios a los efectos de la transmisión de una comunicación, entre otras disposiciones.

3. Acciones Internacionales en contra del *Spam*

En cuanto a la participación internacional sobre la materia de *Spam,* tenemos en primer término a la OECD, que en el 2003 implementó la Task Force on Spam, la cual ha creado grupos de trabajo sobre este tema (Workshop sobre el *Spam*), y sus objetivos van encaminados a dar una repuesta internacional en las distintas políticas y a coordinar la lucha contra el *Spam*, alentado y promoviendo medidas para combatir el *Spam* y códigos de buenas prácticas en el sector de la industria y negocio, así como facilitar la aplicación de las leyes fronterizas.

Esta Organización ha celebrado dos sesiones (Task Force on Spam), celebradas en Bruselas y Busan, en la que participaron tanto autoridades de regulación como representantes del sector privado, para analizar los aspectos técnicos y socioeconómicos del *Spam* y en la que se puntualizaron tres posibles vías para la lucha contra este fenómeno:

- Regulación y control por parte de las autoridades nacionales.
- Autorregulación por parte de la industria (de los ISPs).
- Iniciativas que abarcan la educación de empresas y usuarios de la red, que incluye generar conciencia sobre el problema entre los usuarios y el establecimiento de buenas prácticas de uso en relación con el correo electrónico.

Otra organización que ha intervenido contra el *Spam*, es la Unión Internacional de Telecomunicaciones (UIT), que es el organismo de las Naciones Unidas, encargado de dirigir la Organización de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), la cual ha participado en acciones de cooperación internacional con el objetivo de generar confianza y seguridad en la utilización de las TIC, así como en la elaboración de iniciativas

en la lucha Anti-Spam y lograr acuerdos de cooperación en materia de internet y financiación.

Por lo que hace a la CMSI, ha llevado a cabo en una primera fase la reunión celebrada en Ginebra en julio de 2004, la cual tuvo la participación de 175 países, organizaciones internacionales, representantes de empresas privadas y miembros de la sociedad civil, y de la cual se derivó la Declaración de Principios y un Plan de Acción en esta materia, contemplando ya en una segunda fase (que se llevará acabo en noviembre de este año en Túnez), poner en marcha este Plan.

Su Declaración de Principios[40], señala que "su fundamento esencial de la Sociedad de la Información, y según se estipula en el Artículo 19 de la Declaración Universal de Derechos Humanos, es que todo individuo tiene derecho a la libertad de opinión y de expresión, que este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir información y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. La comunicación es un proceso social fundamental, una necesidad humana básica y el fundamento de toda organización social".

También menciona entre otras cosas, que una infraestructura de red y de aplicaciones tecnológicas, acelera el progreso económico y social de los países y de su gente (B2 22.) que para que los usuarios o consumidores sientan un clima de confianza y seguridad de la información y de las redes, se debe de poner en poner en práctica una cultura global de ciberseguridad (B5). Y al respecto dispone sobre el spam en su artículo 37: "El envío masivo de mensajes electrónicos no solicitados ("spam") es un problema considerable y creciente para los usuarios, las redes e Internet en general. Conviene abordar los problemas de la ciberseguridad y "spam" en los planos nacional e internacional, según proceda".

[40] Véase documento WSIS-03/GENEVA/4-S
http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161%7C1160

En particular podemos decir, que a través de esta Sociedad de la Información se pretende que las TIC, estén al alcance de todo el mundo y fomenta la ciberseguridad para combatir todo aquello que entorpezca su objetivo, como lo es el *Spam*.

El Plan de Acción[41], contempla dentro de sus Líneas de Acción en su Art. 12 del apartado C5 (Creación de confianza y seguridad en la utilización de las TIC), en particular inciso d. en materia de *Spam*, lo siguiente:

"La confianza y la seguridad son unos de los pilares más importantes de la Sociedad de la Información.

a. Propiciar la cooperación entre los gobiernos dentro de las Naciones Unidas, y con todas las partes interesadas en otros foros apropiados, para aumentar la confianza del usuario y proteger los datos y la integridad de la red; considerar los riesgos actuales y potenciales para las TIC, y abordar otras cuestiones de seguridad de la información y de las redes.
b. Los gobiernos, en cooperación con el sector privado, deben prevenir, detectar, y responder a la ciberdelincuencia y el uso indebido de las TIC, definiendo directrices que tengan en cuenta los esfuerzos existentes en estos ámbitos; estudiando una legislación que permita investigar y juzgar efectivamente la utilización indebida; promoviendo esfuerzos efectivos de asistencia mutua; reforzando el apoyo institucional a nivel internacional para la prevención, detección y recuperación de estos incidentes; y alentando la educación y la sensibilización.
c. Los gobiernos y otras partes interesadas deben fomentar activamente la educación y la sensibilización de los usuarios sobre la privacidad en línea y los medios de protección de la privacidad.
d. Tomar medidas apropiadas contra el envío masivo de mensajes electrónicos no solicitados ("spam") a nivel nacional e internacional.

[41] Véase documento WSIS-03/GENEVA/DOC/0005 idem.

e. Alentar una evaluación interna de la legislación nacional con miras a superar cualquier obstáculo al uso efectivo de documentos y transacciones electrónicas, incluido los medios electrónicos de autenticación.
f. Seguir fortaleciendo el marco de confianza y seguridad con iniciativas complementarias y de apoyo mutuo en los ámbitos de la seguridad en el uso de las TIC, con iniciativas o directrices sobre el derecho a la privacidad y la protección de los datos y de los consumidores.
g. Compartir prácticas óptimas en el ámbito de la seguridad de la información y la seguridad de las redes, y propiciar su utilización por todas las partes interesadas.
h. Invitar a los países interesados a establecer puntos de contacto para intervenir y resolver incidentes en tiempo real, y desarrollar una red cooperativa entre estos puntos de contacto de forma que se comparta información y tecnologías para intervenir en caso de estos incidentes.
i. Alentar el desarrollo de nuevas aplicaciones seguras y fiables que faciliten las transacciones en línea.
j. Alentar a los países interesados a que contribuyan activamente en las actividades en curso de las Naciones Unidas tendentes a crear confianza y seguridad en la utilización de las TIC.

Además de la cooperación internacional en la lucha contra el *Spam* ya comentada, también existen acuerdos celebrados entre diversos sectores como lo es el Acuerdo de Entendimiento (Memorandum of Understanding MoU) entre la FTC y la AEPD, de ayuda mutua para facilitar el cumplimiento de la legalidad en materia de correo electrónico comercial, firmado en Washington D. C. en octubre de 2004, y al que se unieron las autoridades del Reino Unido, México y Australia, que tiene por objeto facilitar actuaciones administrativas de cooperación y sin que se establezcan obligaciones legales entre las partes, previendo acciones de ayuda y cooperación bilateral: Asistencia técnica, actualización permanente de modificaciones y novedades legislativas, colaboración con las universidades y promoción de buenas prácticas en los sectores implicados, así como la colaboración y asistencia mutua en las investigaciones sobre *Spam*, dentro de los sus

respectivos marcos legales. A pesar de tener estas acciones, desde nuestro punto de vista, consideramos que para que estas sean más efectivas, se requiere que la lucha antispam sea en forma coordinada, unificando medidas de seguridad y sanciones entre los diversos sectores (naciones, empresas y sociedad en general).

Capítulo IV Regulación Jurídica en México del *Spam*

1. Procuraduría Federal del Consumidor (PROFECO) y Policía Federal Preventiva (PFP)

A pesar de que en nuestro País no contemos aún con un marco regulatorio bien definido sobre la protección de datos y en particular de normas en contra del *Spam*, tenemos distintas autoridades que realizan acciones en contra de esta problemática. Una de ellas es la Procuraduría Federal del Consumidor (PROFECO), que forma parte del Comité de Políticas del Consumidor (CCP) de la OCDE, el cual se encarga del análisis de tendencias en el comercio internacional y propicia la coordinación y cooperación entre los Estados miembros en la lucha contra el abuso hacia los consumidores en las transacciones comerciales en línea.

Este Comité adopto los lineamientos para la protección al consumidor en el contexto del comercio electrónico así como los lineamientos para proteger a los consumidores de prácticas comerciales transfronterizas, fraudulentas y engañosas, promulgados por la OCDE, mencionando entre sus puntos más relevantes:

1) Procurar que las agencias gubernamentales de protección al consumidor cooperen entre ellas para combatir las prácticas comerciales abusivas y engañosas transfronterizas;
2) Procurar la cooperación con el sector privado a efecto de combatir las prácticas fraudulentas y engañosas;

respectivos marcos legales. A pesar de tener estas acciones, desde nuestro punto de vista, consideramos que para que estas sean más efectivas, se requiere que la lucha antispam sea en forma coordinada, unificando medidas de seguridad y sanciones entre los diversos sectores (naciones, empresas y sociedad en general).

Capítulo IV Regulación Jurídica en México del *Spam*

1. Procuraduría Federal del Consumidor (PROFECO) y Policía Federal Preventiva (PFP)

A pesar de que en nuestro País no contemos aún con un marco regulatorio bien definido sobre la protección de datos y en particular de normas en contra del *Spam*, tenemos distintas autoridades que realizan acciones en contra de esta problemática. Una de ellas es la Procuraduría Federal del Consumidor (PROFECO), que forma parte del Comité de Políticas del Consumidor (CCP) de la OCDE, el cual se encarga del análisis de tendencias en el comercio internacional y propicia la coordinación y cooperación entre los Estados miembros en la lucha contra el abuso hacia los consumidores en las transacciones comerciales en línea.

Este Comité adopto los lineamientos para la protección al consumidor en el contexto del comercio electrónico así como los lineamientos para proteger a los consumidores de prácticas comerciales transfronterizas, fraudulentas y engañosas, promulgados por la OCDE, mencionando entre sus puntos más relevantes:

1) Procurar que las agencias gubernamentales de protección al consumidor cooperen entre ellas para combatir las prácticas comerciales abusivas y engañosas transfronterizas;
2) Procurar la cooperación con el sector privado a efecto de combatir las prácticas fraudulentas y engañosas;

3) Procurar que las agencias de protección al consumidor mantengan un constante intercambio de información y experiencias en torno a tales prácticas;
4) Mejorar la capacidad de protección a consumidores extranjeros que han sido engañados por defraudadores nacionales y viceversa.
5) Asegurar un resarcimiento efectivo de los consumidores afectados;
6) Contemplar la posibilidad de realizar investigaciones conjuntas entre países sobre casos fraudulentos y engañosos;
7) Revisar los marcos jurídicos nacionales con objeto de analizar si la legislación nacional cuenta con las herramientas legales pertinentes para combatir este tipo de prácticas.
8) Orientar al consumidor sobre este tema a fin de fomentar una cultura preventiva[42].

Por lo que la publicidad y el marketing deberán de ser honestos y deberá de abstenerse los proveedores de realizar prácticas que sean falsas, fraudulentas, engañosas o dudosas hacia los consumidores, y que en materia de correo electrónico no solicitado, cada país lo autorregulará.

En este aspecto únicamente tenemos que en el año 2000, se incluyó un capítulo (VIII BIS, Art. 76 Bis) de la Ley Federal de Protección al Consumidor de México, el cual determina la protección a la confidencialidad de la información proporcionada por el consumidor en las operaciones que se realicen en línea, como también la obligación por parte de los proveedores de proporcionar los datos de su empresa así como las características de los productos, sus precios y demás condiciones; la prohibición de realizar practicas engañosas hacia el consumidor y el respetar la decisión por parte del consumidor de no recibir avisos comerciales, absteniéndose de utilizar estrategias de venta o publicitarias no claras y que estas incorporen mecanismos que informen que sus contenidos no son aptos para la población vulnerable como los son los niños, ancianos y enfermos[43]:

[42] "Directrices de la OCDE para la protección de los consumidores de prácticas comerciales" s/f. http://www.profeco.gob.mx/html/internacionales/prevfrau/fraude3.pdf (Oct. 28, 2005)
[43] "Ley Federal de Protección al Consumidor" s/f. http://www.ordenjuridico.gob.mx (Oct. 28, 2005)

ARTICULO 76 bis.- Las disposiciones del presente capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

I. El proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente.

II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;

III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;

IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que deriven de ella;

V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, (en su caso), y formas de pago de los bienes y servicios ofrecidos por el proveedor;

VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y

VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población"[44].

Es importante comentar que la fracción VI, del anterior artículo se le deja al consumidor la libertad de decidir que tipo de avisos comerciales desea recibir, y que esta disposición se asemeja al sistema *opt-in* que contempla la Directiva de la Unión Europea 2002/ 58/CE que ya comentamos en el capítulo anterior, pero resulta inconclusa ya que no cuenta con una normatividad que establezca un mecanismo claro y adecuado para que se cumpla con este derecho del consumidor.

En febrero de 2004 se adicionaron nuevas reformas en cuanto a la protección del consumidor en esta ley, las cuales consisten en proteger la privacidad de sus datos personales proporcionados por el consumidor y al no ser molestado por ningún medio para ofrecerle publicidad de cualquier índole si el no lo autoriza, como también el que no se utilicen sus datos con otro propósito más que para el que fueron requeridos por los proveedores, entre las cuales mencionaremos las siguientes:

"ARTÍCULO 1.-…
Son principios básicos en las relaciones de consumo:
…
VII. La protección contra la publicidad engañosa y abusiva, métodos comerciales coercitivos y desleales, así como contra prácticas y cláusulas abusivas o impuestas en el abastecimiento de productos y servicios.

[44] Adicionada en febrero de 2004.

VIII. La real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados, y…”.

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”.

Y contempla la imposición de sanción con multa que van desde $300.00 m. n. a $960,000.00 m. n[45], cantidades que son mínimas en comparación al daño que se ocasiona al comercio electrónico cada año.

Teniendo que estas son las únicas disposiciones que se utilizan por medio de la PROFECO, para el combate en contra del correo no solicitado.

Esta procuraduría también participa desde 1994 con la Red Internacional de Protección al Consumidor y de Aplicación a la Ley (International Consumer Protection and Enforcement Network ICPEN), la cual tiene como actividad principal la protección a los consumidores de prácticas transfronterizas engañosas y fraudulentas (Scam), realizando una serie de acciones para detectar junto con los miembros de la OCDE y representantes de la Comunidad Europea. Esta red entre otras actividades que lleva acabo, organiza los denominados Sweep Days o días de limpieza, los cuáles consisten en detectar todos aquellos sitios que no cumplen con los lineamientos establecidos de la OCDE, para poner en alerta a los consumidores y autoridades[46], y emprender acciones en contra de ellos para mejorar la información que circula en la Web, llevándose a cabo el último los días 21 y 22 de Febrero de este año, en donde México participo activamente junto con la Comisión Federal para la Defensa de los Usuarios de Servicios Financieros (CONDUSEF), y de empresas privadas como Microsoft México, T1msn y NIC México, como de la Asociación Mexicana de Internet (AMIPCI), y de la Universidad Autónoma de México a través de la Dirección General de Cómputo Académico.

Otra autoridad que participa en el combate antispam es la Policía Federal Preventiva, a través de la Policía Cibernética la cual tiene a su cargo las siguientes acciones:

- Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como a la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.

[45] Art. 127 Ley Federal de Protección al Consumidor
[46] "International Internet Sweep Day" s/f. http://www.icpen.org/activities.htm (Oct. 28, 2005)

- Análisis y desarrollo de investigaciones de campo sobre actividades de organizaciones locales e internacionales de pedofília, así como de redes de prostitución infantil.
- Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos utilizando computadoras.
- Realización de operaciones de patrullaje anti-hacker, utilizando Internet como un instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en la red.
- Como resultado del crecimiento de delitos informáticos, la Policía Cibernética de la PFP, asumió el cargo de la Secretaría Técnica del Grupo de Coordinación Interinstitucional de Combate a Delitos Cibernéticos en México, a través de la cual se promueve una cultura de legalidad, respeto y seguridad en la red[47].

Esta autoridad junto con otros organismos internacionales intercambia información para el ataque de delitos cibernéticos como el phishing, scam, spam, entre otros y realiza los denominados patrullajes en la red para identificar sitios con contenido pornográfico y fraudulento así como localizar a las personas que se dedican a cometer estos ilícitos, con la finalidad de ofrecer seguridad en el ciberespacio a los usuarios de Internet.

2. Propuestas Legislativas en materia del *Spam*.

En virtud del daño que ocasiona la práctica de envíos masivos de correos no solicitados, en el contexto del Congreso de la Unión se han presentado dos propuestas para regular y delimitar la práctica del *Spam*, mismas que han sido analizadas y revisadas primero por la

[47]"Conoce a la policía cibernética" s/f. http://www.ssp.gob.mx/application?pageid=pcibernetica_sub_1&rootId=126&pbname=pc_conoce (Oct. 28, 2005).

Cámara de Senadores y posteriormente han sido turnadas a la Cámara de Diputados, estando ambas pendientes de su aprobación.

La primera de ellas es la iniciativa del Diputado Julio César Córdova Martínez, que propone para que se reformen y adicionen 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)*[48].

Por lo que hace a la Ley Federal de Protección al Consumidor, en su proyecto señala que no se considerará correo no solicitado:

1.- 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;

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

3.- 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;

4.- 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;

5.- Cuando el mensaje tenga por objeto proporcionar de forma regular y periódica, información concerniente a cambios de estado, situación u otros reportes del destinatario

[48] Ver anexo 2.

respecto a suscripciones, membresías, cuentas, préstamos o cualesquiera otras relaciones análogas corrientes con el remitente;

6.- 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.

7.- 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.

Y delimita ciertas condiciones para la protección de los destinatarios como el señalar claramente el asunto de que se trate el correo, y que no contengan información que hagan caer en el error con encabezados, origen o destino falsos, y que se le permita al remitente manifestar su voluntad de recibir correos subsecuentes en su cuenta, y de no cumplirse estas condiciones, se hará acreedor a sanciones administrativas previstas en la misma ley. Propone la adición de una fracción en el Art. 76 Bis (VIII), para la información cuyo contenido sea solo para adultos especifique claramente que es no es apta para menores como las leyendas: “contenido exclusivo para adultos”.

Para la materia penal, establece la iniciativa, la adición de un capítulo (III), acerca de la Remisión Masiva de Mensajes de Datos Ilícitos por Correo Electrónico en el Código Penal Federal. Señalando que se considerara como 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, y por mensajes de datos ilícitos:

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.

Se impondrán de uno a cinco años de prisión y de ciento cincuenta a ciento cincuenta mil días y propone que estos delitos se persigan por querella del ofendido, cuestión que no permitiría la efectividad de estas modificaciones propuestas por el Diputado, ya que desde nuestro punto de vista, si estos delitos se persiguieran de oficio por parte de las autoridades penales, reforzaría las acciones antes expuestas, que lleva a cabo tanto la PROFECO como la PFP a través de la policía cibernética, para la detección de publicidad y sitios que llevan al usuario a información engañosa.

En cuanto a lo que señala la iniciativa para la Ley Federal de Telecomunicaciones, propone que se contemplen también estas remisiones masivas de mensajes de datos ilícitos por correo electrónico, en el contexto de esta ley para que puedan ser sancionadas.

La segunda propuesta, es la que expide la Ley Federal que regula el correo electrónico, presentada por el Diputado Jorge Legorreta Ondorica, del grupo parlamentario del PVEM[49], el 29 de septiembre de 2004.

Entre lo más destacable de esta iniciativa de ley, podemos mencionar que en su Art. 1 dispone lo siguiente:

"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."

Para esta iniciativa, no se considera *Spam*, toda publicidad de productos o servicios con cualquier contenido (cadenas, pornográfico, comercial, etc.) si el receptor lo solicito, y se le da la facultad de retirar su consentimiento en cualquier momento, en el caso de que el remitente continúe haciéndolo se considerara como correo no solicitado. Punto que nos parece importante, ya que el receptor es libre de determinar que tipo de información desea recibir, ya que habrá usuarios que les interese obtener información por ejemplo de la compra de viajes y que sea el mismo quien la solicite y no que en cualquier momento su bandeja de correo se vea saturada de correos que contengan información que el no desee y le entorpezca la entrada de mensajes que espera recibir.

De igual manera, delimita las prohibiciones que se tiene en el entorno a esta práctica nociva entre las que destacan:

1.- Acceder a una computadora protegida, sin autorización o con otro servicio de acceso al público a Internet, para que por medio de estas, se inicie la transmisión o envío de múltiples

[49] Ver Anexo 3.

mensajes de correos tipo *Spam*, o para retransmitir mensajes con la finalidad de engañar o mal informar a los receptores, y alterar la información en los títulos del correo en línea para enviar este tipo de mensajes.

2.- No se podrá usar información que falsifique la identidad de una persona, para que se registren varias cuentas de correo o hacerse pasar por un prestador de algún servicio de Internet, o comercializar listas de correos o realizar combinaciones de cuentas o de prestadores de servicios de Internet.

3.- No deberá presentarse el remitente ante los receptores como legítimo prestador de servicios de Internet, u obtener direcciones de correo electrónico, sin su consentimiento cualquier sistema automatizado o software, de cualquier conexión a Internet que se encuentre dentro del territorio nacional o bien generar direcciones con combinaciones de nombres, letras o números para el envío de *Spam.*

4.- Promover, enviar o admitir la promoción de productos o servicios a través de este tipo de correo para obtener una ganancia ilícita con información falsa o engañosa para llevar a cabo algún negocio; así como también el envío de información con material, imágenes con contenido sexual.

Así mismo propone integrar una Comisión de Regulación del correo electrónico tipo *Spam,* presidida por la Secretaría de Comunicaciones y Transportes por medio de la cual se llevaría el registro de los remitentes reportados por los receptores o que sean detectados por la Comisión a través de los rastreos que lleven acabo; podrá realizar investigaciones de oficio o basadas en denuncias o quejas ante el Agente del Ministerio Público Federal, para que sean sancionadas estas prácticas.

En materia de sanciones, esta iniciativa, establece empatar estas prácticas con disposiciones ya previstas en el Código Penal Federal y el Código de Procedimientos Penales.

Con esta propuesta, podemos decir, que en comparación con la del Diputado Julio César Córdova Martínez, que propone el cambio o adhesión en varias leyes, esta iniciativa pretende que una ley sea exclusivamente para legislar esta problemática y mejor aun de competencia federal, además podría estar acorde con lo que han dispuesto organismos internacionales, lo cual estandarizaría las disposiciones jurídicas a nivel internacional y traería aparejada la modificación de varias leyes nacionales, como las que hemos mencionado anteriormente para que en su conjunto se logre tener una regulación jurídica nacional del *Spam*.

Conclusiones

I. En virtud del desarrollo del Comercio, tenemos que la práctica comercial tradicional no representaba una amenaza de la intimidad de los consumidores, y que con los avances tecnológicos, las empresas poseen nuevas herramientas para llegar al consumidor a través de una nueva forma de hacer comercio denominado comercio electrónico o en línea a través de internet.

II. Este tipo de comercio trae consigo grandes ventajas, entre otras agiliza las operaciones mercantiles a distancia y ha abierto mercados, con bajos costos para las empresas y particulares, ofreciendo como principales servicios el intercambio de información, utilización de la web y del correo electrónico el cual permite y facilita la comunicación entre personas de cualquier parte del mundo.

III. Pero este comercio, no ha sido del todo bueno, ya que en virtud de su rápida expansión, la regulación jurídica no se ha desarrollado a la par por lo que encontramos prácticas fraudulentas y engañosas como es el correo electrónico no deseado o *Spam*.

IV. El cual como lo hemos desarrollado, en un primer plano ocasiona daños a los usuarios en lo económico, pérdida de tiempo y afectación de su intimidad, y en mayor escala provoca la poca confianza para realizar operaciones comerciales en línea y con ello grandes pérdidas económicas hacia las empresas, siendo que internet es una herramienta que entre otras cosas, apoya al crecimiento en el entorno económico.

V. El combate antispam requiere que tanto la tecnología como la legislaciones trabajen conjuntamente para el desarrollo de estrategias que permitan su implementación efectiva.

VI. En virtud de los daños que ocasiona el *Spam*, es conveniente que en el ámbito internacional, las legislaciones de los países y organismos internacionales sean homogéneas

para que el correo no solicitado, siendo un problema extraterritorial, pueda ser atacado de igual forma en el contexto mundial.

VII. En nuestro país, es necesario en primer término que exista una ley en materia de protección de datos personales ya que al no contar con ella existe una inseguridad en cuanto hace al derecho a la intimidad o privacidad, y propicia el crecimiento de esta práctica nociva.

VIII. En segundo término, ante los daños que ocasiona la práctica del *Spam*, se requiere de una normatividad exclusiva para esta práctica, para que se determine la adopción de un sistema *opt-in* o bien el *opt-out*, como de las condiciones para que sea considerado por nuestras leyes como una práctica ilícita y de esa forma pueda ser sancionada con multas o prisión para los detractores de la ley, con la finalidad de eliminar o bien disminuir el *Spam* en la red.

IX. Es *urgente* y *necesario* que se agilice el proceso legislativo pendiente en el Congreso en estas materias, ya que conforme pasa el tiempo y al no existir una normatividad, los daños internos que sufre nuestro comercio electrónico se han ido acrecentando como también, la inseguridad hacia los usuarios de nuestro país.

Bibliografía

Barnes Vázquez, J. Internet y el Derecho.Una nota acerca de la libertad de expresión e información en el espacio cibernético. Madrid, Ordenación de las Telecomunicaciones, 1997.

Barrios Garrido, Gabriela; Muñoz de A. M., Marcia y Camilo Pérez Bustillo. *Internet y derecho en México.* México, Mc Graw Hill, 1998.

Davara Rodríguez, Miguel Ángel. *La Protección de Datos en Europa.* Madrid, Universidad Pontificia Comillas ICAI-ICADE, 1998.

- *La Protección de Datos personales en el sector de las Telecomunicaciones.* Madrid, Universidad Pontificia Comillas ICAI-ICADE, 2000.

Jijena L., Renato; Palazzi, Pablo A. y Julio Téllez V. *El Derecho y la Sociedad de la Información: la importancia de Internet en el mundo actual*. México, Miguel Ángel Porrúa y Tec de Monterrey, Campus Estado de México. 2003.

Loshin, Pete. *Essential Email Standards: RFCs and Protocols Made Practical*. USA, Wiley, 2000.

McWilliams, Brian. *Spam Kings*. USA, O´Reilly, 2004.

Sarra, Andrea V. *Comercio electrónico y derecho*. Buenos Aires, Astrea, 2000.

Schwartz, Alan. *SpamAssassin*. USA, O´Reilly, 2000.

Schwartz, Alan y Simson, Garfinkel. *Stopping Spam*. USA, O´Reilly, 1998.

Téllez Valdés, Julio. *Derecho Informático*. 3ª. Ed., México, Mc Graw Hill, 2004.

Villanueva, Ernesto. *Derecho de la información*. Quito-Ecuador, CIESPAL, 2003.

Viñamata P., Carlos. *La Propiedad Intelectual*. México, Trillas, 2003.

LEGISLACIÓN:

CAN-SPAM Act. EUA, 2004.
Código Civil Federal. México, Porrúa. 2005.
Código de Comercio. México, Porrúa. 2005.
Código Fiscal de la Federación. México, Porrúa. 2005
Constitución Política de los Estados Unidos Mexicanos. México, Porrúa. 2005.
Código Penal Federal. México, Porrúa. 2005.

Directiva 95/46 del Parlamento Europeo y del Consejo, 1995.
Directiva 2000/31/CE.
Directiva 2002/ 58/CE.
Ley de Instituciones de Crédito. México, Porrúa. 2005.
Ley de Propiedad Industrial. México, Porrúa. 2005.
Ley Federal de Competencia Económica. México, Porrúa. 2005.
Ley Federal del Derecho de Autor. México, Porrúa. 2005.
Ley Federal de Protección al Consumidor. México, Porrúa. 2005.
Ley Federal de Telecomunicaciones. México, Porrúa. 2005.
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. México, Porrúa. 2005.
Ley Estatal de California: Ley contra el correo basura (*antispam)*, 1998.
Ley Orgánica de Protección de Datos (LOPD). España, 1999.
Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSICE 34/2002). España, 2002.

LIGAS DE INTERNET:

http://www.aece.org/legislacion.asp
http://biblioteca.itesm.mx/nav/contenidos_salta2.php?col_id=drae
http://www.cddhcu.gob.mx/
http://www.definicion.org/banner
http://gaceta.cddhcu.gob.mx/
http://gac.icann.org/web/about/gac-outreach_Spanish.htm
http://www.icann.org
http://www.icpen.org/activities.htm
http://www.ifai.org.mx/datos_personales/nacionales.htm
http://www.ifai.org.mx/transparencia/LFTAIPG.pdf
http://www.itu.int/ITU-T/wtsa/resolutions04/S/RES51S.doc
http://www.itu.int/newsroom/press_releases/2005/05-es.html
http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161%7C1160
http://www.itu.int/wsis/index-es.html
http://www.jornada.unam.mx/2005/03/24/019n1eco.php
http://www.juridicas.com/base_datos/Admin/lo15-1999.html
http://www.microsoft.com.mx
http://www.nic.mx
http://www.oecd.org
http://www.ompi.org
http://www.ordenjuridico.gob.mx
http://www.pc-news.com
http://www.profeco.gob.mx/html/estadistica/informe/inf2003/Profeco2003.pdf
http://www.profeco.gob.mx/html/internacionales/prevfrau/fraude3.pdf
http://www.reforma.com/Negocios/spam
http://www.rompecadenas.com.ar/spam.htm
http://www.sice.oas.org/e-comm/legislation/mex2.asp#cont

http://www.spamhaus.org
http://www.spamlaws.com/eu.shtml
http://www.spamlaws.com/federal/can-spam.shtml
http://www.spamlaws.com/state/ca.shtml
http://www.ssp.gob.mx/application?pageid=pcibernetica_sub_1&rootId=126&pbname=pc_conoce
http://www.un.org/spanish/documents/ga/res/51/list51.htm
http://www.uncitral.org/uncitral/es/about/origin.html
http://www.vsantivirus.com/hoax.htm
http://www.vsantivirus.com/scam-loteria.htm
http://www.vsantivirus.com/scam-nigeria.htm
http://www.vnunet.com/news/425551
http://www.wipo.int/portal/index.html.es
http://www.wto.org/spanish/tratop_s/ecom_s/wkprog_s.htm

AUDIOGRÁFICAS:

Domingo Donovan, Mauricio (Cassette).Entrevista. México. 11 hrs., 5 de septiembre, 2005, Microsoft México. 60 min.

OTRAS FUENTES:

Acuerdo de Entendimiento (Memorandum of Understanding - MoU) entre la FTC (Federal Trade Comisión) y la AEPD, de Ayuda mutua para facilitar el cumplimiento de la legalidad en materia de correo electrónico comercial. Comisión Federal de Comercio. 2004.

Acuerdo sobre los Aspectos de los Derechos de la Propiedad Intelectual Relacionados con el Comercio (ADPIC).

Declaración sobre el Comercio Electrónico Mundial adoptada por los Ministros en el segundo período de sesiones de la Conferencia Ministerial se insta Consejo General. 1998, WTO.

Declaración de Principios de la CMSI WSIS-03/GENEVA/4-S.

Declaración Universal de los Derechos Humanos.

Convenio 108 del Consejo de Europa para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales. 1981.

Iniciativa de ley sobre la protección de Archivos privados del 30 de Abril de 2002, presentada por el Senador Antonio García Torres. Gaceta Parlamentaria.

Iniciativa que expide la Ley Federal que regula el correo electrónico, presentada por el Diputado Jorge Legorreta Ordorica, del grupo parlamentario del PVEM, en la sesión del miércoles 29 de septiembre de 2004, publicada en la Gaceta Parlamentaria, año VII, número 1595, jueves 30 de septiembre de 2004.

Ley Modelo sobre el Comercio electrónico. UNCITRAL. 1996.

Recomendación del Consejo, relativa a los Lineamientos para la protección al Consumidor en el Contexto del Comercio Electrónico. 1999, OECD.

Reforma que 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),* a cargo del Diputado Julio César Córdova Martínez, del grupo parlamentario del PRI. Publicada en la Gaceta Parlamentaria, número 1737-II, jueves 21 de abril de 2005.

Resolución sobre los Lineamientos para proteger a los consumidores de prácticas comerciales fraudulentas y engañosas a través de las fronteras. OECD. 2003

Plan de Acción de la CMSI WSIS-03/GENEVA/DOC/0005.

Tratado de Libre Comercio de América del Norte (TLCAN), Capítulo XVII relativo a la Propiedad Intelectual.

Anexos

Anexo 1

Ejemplos de *Spam*

1. Fraude Nigeriano

From:Dr.Malenge Uwa
Tel:44-790-346-3032(Satellite teléfono).
Lagos-Nigeria.
Email:uwa9800@email.com OREGON uwa9800c@mailcity.com(confidencial)

Attn:President/Ceo.

PROPUESTA COMERCIAL ESTRICTAMENTE CONFIDENCIAL
REF: TRANSFERENCIA DE US$21.5 MILLONES (VEINTE UN MILLONES, QUINIENTOS MIL DOLARES AMERICANOS).

Yo sé que este email lo tomará como una sorpresa, pero no necesita preocuparse como nosotros estamos usando el único medio asegurado y confidencial disponible para buscar ayuda y un socio extranjero en un negocio de transacción que es de beneficio mutuo.

Yo soy un miembro del Gobierno Federal de Nigeria Contract Award and Monitoring Committee in the Nigeria National Petroleum (NNPC).

Hace un tiempo, un contrato fue otorgado a una empresa extranjera en NNPC por mi Comité. Este contrato finalizó facturando una suma de US$21.5M dólares americanos. Esto fue hecho deliberadamente. El sobre facturar era un trato hecho por mi comité para beneficiarnos del proyecto. Nosotros queremos transferir este dinero de la cuenta en que ahora está, una cuenta suspendida con el NNPC, a una cuenta de cualquier extranjero, como la suya.

Por ayudarnos en este trato, usted se hará acreedor al 30% del dinero, 60% será para mi y mis socios, mientras que el 10% será usado para cubrir cualquier gasto relacionado con los trámites del traslado. Puede interesarle saber que una transacción similar era llevada a cabo por MR. PATRICE MILLER, President of Crane International Trading Corp. of 153 East 57th St., 28th floor, NY10022, TEL:(212)-308-7788 AND TELEX: 6731689.

El trato ha concluido, y todos los documentos necesarios fueron remitidos al Sr. Miller para autentificar su demanda. Una vez que los fondos fueron transferidos, el Sr. Miller presentó a su banco todos los documentos legales y remitió todos sus fondos a otra cuenta para luego desaparecer completamente, con su dinero claro.

La información anterior se usa para hacer una explicación formal en el procedimiento del traspaso de dinero. No importa si su compañía hace proyectos de contratos de esta naturaleza o no. La idea es que su empresa ganó el contrato mayor y lo subcontrató fuera del país a otras compañías.

Muy a menudo grandes compañías comerciales ganan grandes contratos que luego subcontratan a empresas más especializadas para su ejecución.

Nosotros tenemos conexiones fiables fuertes y contactos en el Banco Central de Nigeria, así como en el Ministerio Federal de Finanzas y nosotros no tenemos duda de que todo el dinero será liberado y transferido, si conseguimos el socio extranjero necesario para ayudarnos en este trato. Por consiguiente, cuando el negocio sea concluido con éxito nosotros enviaremos todos los documentos conseguidos a través de esos contactos, por todos los ministerios de gobierno para tener un 100% de seguridad.

Nosotros somos servidores civiles ordinarios, y no queremos que esto se confunda con un oportunidad de hacerse rico. Queremos transferir este dinero a un banco elegido por nosotros, antes que nuestro actual gobierno democrático comienza a auditorear a todas las empresas paraestatales usadas por el Gobierno Federal.

Por favor avíseme inmediatamente a través de mi dirección de email confidencial si usted está interesado o no en este negocio. Si está interesado, envíe los documentos requeridos, necesarios para este negocio.

Yo aguardo su colaboración más plena en este negocio.

Fielmente suyo,
Dr.Malenge Uwa.

http://www.vsantivirus.com/scam-nigeria.htm (Oct.15, 2005)

2. Estafa del premio de la Lotería

De: "INTERNATIONALLOTTERYINC"
<internationallotteryinc@rediffmail.com>
Asunto: CONGRATULATIONS!!!YOU'VE WON.

INTERNATIONAL LOTTERY INC.

FROM:THE DESK OF THE VICE PRESIDENT
INTERNATIONAL LOTTERY INC/PRIZE AWARD DEPT.
Ref. Number:EGS/2551256012/02
Batch Number:14/0017/1PD
ATTENTION.

Sir/Ma/Miss,

We are pleased to inform you of the result of the winners of the International Lottery programs held on the 15th March,2003.Your e-mail address attached to ticket number 025--11464992--750 with serial number 2113--05 drew lucky numbers 8-10-23-30-32-49 which consequently won in the 3rd category.You have therefore been approved for a lump sum pay of US$ 150,000.00(One hundred and fifty thousand United States Dollars) in cash credited to file REF NO:EGS/2551256012/02.This is from a total cash prize of US $2.250.000.00(Two million two hundred and fifty thousand dollars)shared among the fifteen international winners in this category.

CONGRATULATIONS!!!

Due to mix up of some numbers and names we ask that you keep your winning information confidential until your claims has been processed and your money Remitted to you.This is part of our security protocol to avoid double claiming and unwarranted abuse of this program by some participants.

All participants were selected through a computer ballot system drawn from over 20,000 company and 30,000,000 individual email addresses and names from all over the world.This promotional program takes place every three years,the lottery was promoted and sponsored by the President of the World Largest software,Bill Gates.We hope with part of your winning you will take part in our next year USD 50 million international lottery.To file for your claim please contact our financial agent,Foriegn operations manager ERIK MOORE of the Macarthy Finance Trust Security Services with your telephone and fax numbers.

TEL:0031-630118250
FAX:0031-645678572

Remember all winning must be claimed not later than 12th of May 2003. After this date all unclaimed funds will be included in the next stake. Please note in order to avoid unnecessary delays and complications please remember to quote your reference number and batch numbers in all correspondence.Furthermore,should there be any change of address do inform our agent as soon as possible.

Congratulations once more from our members of staff and thank you for being part of our promotional program.

Note: Anybody under the age of 18 is automatically disqualified.

Sincerely yours,

KATTY GARCIA.
Lotto Co-ordinator

http://www.vsantivirus.com/scam-loteria.htm (Oct.15, 2005)

Anexo 2

Propuesta Legislativa en materia de *Spam*

Diputado Julio César Córdova Martínez

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),* A CARGO DEL DIPUTADO JULIO CÉSAR CÓRDOVA MARTÍNEZ, DEL GRUPO PARLAMENTARIO DEL PRI[50]

El suscrito, diputado federal de la LIX Legislatura del honorable Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos y 55, fracción II, 56 y 62 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, someto a la consideración del Pleno de la Cámara de Diputados la presente Iniciativa con Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Protección al Consumidor, del Código Penal Federal y de la Ley Federal Telecomunicaciones, conforme a la siguiente

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

[50] Publicada en la Gaceta Parlamentaria, número 1737-II, jueves 21 de abril de 2005. http://gaceta.cddhcu.gob.mx/ (Oct. 5 2005)

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.

Transitorio Único. Este decreto entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Dip. Julio César Córdova Martínez (rúbrica)

Anexo 3

Propuesta Legislativa en materia de *Spam*

Diputado Jorge Legorreta Ordorica

QUE EXPIDE LA LEY FEDERAL QUE REGULA EL CORREO ELECTRÓNICO, PRESENTADA POR EL DIPUTADO JORGE LEGORRETA ORDORICA, DEL GRUPO PARLAMENTARIO DEL PVEM, EN LA SESIÓN DEL MIÉRCOLES 29 DE SEPTIEMBRE DE 2004[51]

Jorge Legorreta Ordorica, diputado de la LIX Legislatura del H. Congreso de la Unión, integrante del grupo parlamentario del **Partido Verde Ecologista de México**, con fundamento en los artículos 71, fracción II, 72 y 73, fracción XVII, de la Constitución Política de los Estados Unidos Mexicanos; 26 de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; y 55, fracción II, 56, 60 y 64 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, solicito se turne **a la Comisiones de Comunicaciones, y de Ciencia y Tecnología,** para su dictamen y posterior discusión en el Pleno de la Cámara de Diputados de la Quincuagésima Novena Legislatura del Honorable Congreso de la Unión, la siguiente iniciativa con proyecto de decreto.

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,

[51] Publicada en la Gaceta Parlamentaria, año VII, número 1595, jueves 30 de septiembre de 2004. http://gaceta.cddhcu.gob.mx/ (Oct. 5, 2005)

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:

Decreto que expide la Ley Federal que Regula el Correo Electrónico

Artículo Único. se expide la Ley Federal que Regula el Correo Electrónico, para quedar como sigue:

I**niciativa 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.

Prohibiciones

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.

De la Comisión de Regulación del Correo Electrónico Tipo *Spam*

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*.

De las Sanciones

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.

Transitorios

Primero.- La presente ley entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

Segundo.- El Ejecutivo Federal tendrá un plazo de noventa días, a partir de la publicación de la presente ley, para expedir el Reglamento respectivo, en el que se incluirá la creación de la Comisión a que se refiere el artículo 19 de la presente ley.

Dado en el Palacio Legislativo de San Lázaro, Sede de la Cámara de Diputados del Honorable Congreso de la Unión de los Estados Unidos Mexicanos, a los 29 días del mes de septiembre de 2004.

Diputados: Manuel Velasco Coello, coordinador; Jorge A. Kahwagi Macari, vicecoordinador; Luis Antonio González Roldán, vicecoordinador; Francisco Xavier Alvarado Villazón (rúbrica), Leonardo Álvarez Romo, Jacqueline Argüelles Guzmán, María Ávila Serna, Fernando Espino Arévalo, Maximino Fernández Ávila, Félix Adrián Fuentes Villalobos, Alejandro Agundis Arias, Jorge Legorreta Ordorica (rúbrica), Julio Horacio Lujambio Moreno, Alejandra Méndez Salorio, Cuauhtémoc Ochoa Fernández (rúbrica), Javier Orozco Gómez (rúbrica), Raúl Piña Horta.

(Turnada a la Comisión de Comunicaciones. Septiembre 29 de 2004.)

Apéndice Único

Entrevista realizada al Director Jurídico de Microsoft México, Mauricio Domingo Donovan, el 5 de Septiembre de 2005.

Sonia Lazcano (SL): ¿Que daños ocasiona el *Spam* en México?
Mauricio Domingo (MD): Por arriba del 70% de los correos electrónicos que hay en la red hoy son Spam, son correos basura, y ya cada día ves más información sobre el *Spam*. Hay dos tipos de daños o dos frentes de daños fundamentales:
Primero es en el usuario, el tiempo productivo que invierte una persona para depurar su correo electrónico tiene un costo, que es adverso a la competitividad ya sea de un profesionista o de las empresas que contratan a esos profesionistas, entonces se calcula mas o menos que va subiendo, pero el promedio una persona normal invierte es de 45 minutos de su día depurando su correo electrónico. Y esto tiene un costo inmediato relacionado, independientemente del acto de molestia de los *Spams* que pueden ser o no éticos o no morales o inclusive que puedan contener un acto de actividad delictiva como insertar algún virus o algún spyware o este defraudar a los usuarios que es el Scam.

Otro daño es el también monetario, y es mucho mayor y es que los ISP (Los proveedores del servicio de Internet), tienen que invertir recursos para cumplir con sus niveles de servicio, entonces si tu contratas con algún proveedor de servicios de internet y se compromete a darte una velocidad de X, de lo que sea, pues para poder hacer eso y no verse afectados por el *Spam*, pues tienen que meter servidores adicionales gratis que tienen un costo y el problema del *Spam* no es emisor ni receptor si todos van a llegar a un lugar sería fenomenal pero el 80% del *Spam* que se envía no llega a ningún lado entonces esta en la red, porque la maquina tiene como instrucción que un correo tiene que llegar a alguna parte entonces inclusive primero te da un aviso de que no encuentra la dirección pero que no es necesario que lo reenvíes y luego tienes que anotar tu dirección, pero pasan días para que te digan no encontré tu dirección y todo ese tiempo, toda esa onda de tu correo se quedó en la red y eso afecta al ancho de banda, la velocidad y el servicio que da el prestador de servicio, causa desgaste con el consumidor y entonces el ISP tiene que invertir más dinero para que pueda darle el nivel de servicio deseado.

Esos son los daños, los bienes jurídicos a tutelar, la infraestructura y los actos de molestia de una persona en su mismo curso y es un problema grave porque todo el mundo sabe que el e-mail hard destiny se hace mediante un hardware especial, lo usa hackers, trackers, spammers y son direcciones electrónicas al azar como Mauricio Domingo@hotmail.com, lo va creando y alo mejor para una persona: Mauricio Domingo, crea miles de posibles direcciones pero nada màs es una la que yo tengo, entonces esas miles no van a ir a dar a ninguna parte, entonces ese es el daño que se ocasiona y el daño es millonario puede llegar a ocasionar en un extremo.

Afortunadamente, los avances tecnológicos han sido buenos para ir depurando y filtrando el *Spam* pero puede llegar a un extremo que sea inoperable el correo electrónico de tanta basura que lleva y es un habilitador como todas las tecnologías en información un

habilitador de la competitividad en el momento que deja de ser competitivo deja de funcionar.

SL: En el caso de México, ¿cuál es el caso más importante con el que se ha enfrentado Microsoft México respecto a *Spam* judicialmente?

MD: Ninguno porque no hay un marco regulatorio y mientras no haya un marco regulatorio, nosotros no podemos accionar contra un *Spam*. En Microsoft a nivel mundial, hemos tenido muchas historias de éxito en donde nos asociamos con las entidades de procuración de justicia y combatimos *Spam*, porque *Spam* es un negocio millonario, es lo que tiene que entender la gente. Estas gentes cobran medio centavo o un centavo de dólar por cada correo que llega, es un negocio multimillonario para ellos, entonces mientras no exista un marco legislativo en México no podemos accionar en contra de los potenciales spammers que existan, entonces por eso es tan importante empujar un marco legislativo para combatir el *Spam*, en materia administrativa por parte del usuario ni en materia civil y penal por parte de los grandes ISP's, aunado a eso, ten en cuenta que en México nosotros no somos proveedores de internet, tenemos T1msn que es un Joint Venture con Telmex pero es un portal, pero aun así siendo una empresa socialmente responsable y siendo que el fenómeno de *Spam* utiliza mucho el Spuffing y POP nets, si hemos sabido de casos de Spammers que utilizan direcciones de IP de instituciones mexicanas como zoombies o como robots, pero no podemos hacer nada porque no hay un marco regulatorio, en el momento que existan invertiremos recursos y nos acercaremos a las entidades de procuración de justicia para accionar pero mientras no.

SL: Me podría hablar muy brevemente del caso de Microsoft en contra el Rey del *Spam* Scott Richter, cual es su punto de vista en cuanto a la forma de resolver este caso.

MD: Llegamos a un arreglo, tenemos cerca de 350 casos a nivel mundial son muchísimos, por eso no es una pregunta sencilla. El rey del *Spam* se llama Scott Richter y era una compañía que se llama Optimrichtbig.com que estaba basado en Colorado y era la tercera operación ilegal de *Spam* a nivel mundial, en el momento en que Microsoft hizo su demanda en Diciembre de 2003, esta demanda fue en conjunto y en una acción paralela con el procurador del Estado de Nueva York, Elliot Spitspurg y bajo los términos del acuerdo que alcanzamos, Richter y su compañía va a cumplir con toda la regulación antispam en el futuro y pagará siete millones de dólares de daños a Microsoft y está sujeto a la aprobación de la corte, nosotros vamos a reinvertir el monto obtenido por Richter, uno para expandir nuestras actividades de demandas a nivel mundial, usar los recursos para demandar a *Spam*, phishing spyware, explotación de niños, virus y códigos maliciosos y en aprecio al rol que jugamos con la procuraduría del Estado de Nueva York, vamos a poner algunos centros comunitarios digitales en el Estado de Nueva York, para que la gente tanto adultos como niños de recursos no tan privilegiados puedan accesar a la tecnología.
Esto es uno de los primeros casos que llegamos a un acuerdo, es un acuerdo importante y si va a mandar el mensaje correcto a los demás Spammers a nivel mundial.

Microsoft ha colaborado con por lo menos diez entidades de procuración de justicia en Estado Unidos, para entablar demandas en contra de Spammers y Microsoft está apoyando que se cumpla la legislación para parar el *Spam* y otros delitos relacionados con ciber. Estamos trabajando en todos los frentes tanto técnico, colaboramos con entidades de procuración de justicia, inclusive en la parte legal para que el internet sea un lugar menos peligroso para los cibernautas y evidentemente el tener un marco regulatorio para poder llevar a cabo estas acciones son la base para poder llevar este mensaje a los Spammers, hace unos días presentamos un nuevo caso en Florida contra Scout Filard que esta fugado, presentamos como evidencia treinta mil mails para mostrar el delito de *Spam*, y estamos colaborando con los Estados de Washington, Nueva York y Texas para este mismo caso. Estamos trabajando ahorita, en cerca de ciento veinte acciones a nivel mundial de los cuales noventa y seis nada mas son en Estados Unidos y hasta ahorita el único que hemos recolectado es el primero caso que te mencione de Nueva York, pero tenemos sesenta casos que ya están llegando a un acuerdo económico y en donde el monto que se obtenga de ellos se reinvertirán para seguir acciones a nivel mundial.

SL: Que propondría para el combate antispam?

MD: Hay dos iniciativas en la Cámara del Diputado Legorreta (Partido Verde) y la iniciativa del Diputado Julio César Córdova (PRI), nosotros apoyamos la iniciativa del Diputado Córdova, porque consideramos que es muy completa, que es mejor modificar ciertas legislaciones, adicionar ciertos conceptos, que hacer una legislación que regule el correo electrónico, no es nuestra forma de ver las cosas, lo que pasa con el modelo de Legorreta es seguir la legislación europea, y la legislación Europea basa su control de *Spam* en base mucho a privacidad de datos personales, y yo creo que eso es un error porque ojalá y fueran robo de bases de datos en la mayoría del *Spam* porque entonces no pasaría el problema que te comentaba al principio solo los mails llegarían a un destinatario y se acabo el problema a lo mejor y voy a recibir más correo pero desde el punto de vista del ISP, no le afecta tanto y la verdad es que no, la verdad es que el problema viene del e-mail hard destiny, vale mucho más una base de datos que tienes la certeza que existe el usuario final, pero la gran mayoría de los Spammers utilizan este software, entonces no necesariamente hay una relación entre datos personales, privacidad de datos personales y *Spam* son cosas declarables, la segunda cosa no solamente en materia de *Spam*, sino en materia de delitos en general es todo este debate de que hay que hacer código cibernéticos, la verdad es que no los delitos son los mismos, pornografía infantil, fraude, terrorismo, secuestro nada más que el medio es otro y al ser un medio masivo si debería haber una penalización mayor porque es un medio masivo y es accesible a todos, pero la conducta es la misma, o sea si tu matas al alguien con un cuchillo, o con una pistola o con tus manos, sigue siendo el mismo delito de homicidio, nada más que tendrán diferentes agravantes, o sea es lo mismo en este caso, pero la conducta del *Spam* si es una conducta nueva que se tiene que tipificar como delito porque es nueva no existía. Entonces tipificar, para mi solamente existen cuatro delitos: Acceso no autorizado a sistemas (Hacking), *Spam* relacionado Scam y Phishing es fraude son medios para defraudar, Malicious Coule y Spite. Son los cuatro delitos que son netamente cibernéticos, los demás son conductas que ya tipificadas hay que meter un agravante por internet, entonces hay que regular el correo electrónico no solicitado y hay

que regularlo de forma inteligente, entonces la propuesta del Diputado Julio César Córdova es bastante sensata a lo mejor hay que mover los números de cuantos mails mandas al día y todo esto, pero es muy completa en cuanto a que quiere regular el correo electrónico no solicitado y no afectar las actividades de mercadeo directo, porque también es cierto que a mi si me gusta recibir promociones de viajes que tienen en su portal empresas es un correo solicitado, entonces tu tratas con empresas que tienen una política de correo electrónico entonces tu dices no quiero recibirlos y no los recibes y si quieres los recibes, es tan sencillo como eso, el problema no esta con las grandes empresas, con las empresas X, el problema está con otro tipo de empresas que cada vez más si tu analizas el *Spam*, son empresas o que venden piratería o están tratando de defraudar, ya no son empresas establecidas o se están tratando de un Scam o la carta nigeriana, etc. pero ya las empresas establecidas tienen un código de autorregulación, sino hay regulación les da el servicio de lo que este trabajando que funciona bastante bien, entonces ya el correo electrónico no solicitado cada vez más es de empresas con actividades diferentes verdad que es un mercadeo directo para ofrecer productos, precisamente también hace unas semanas o meses anunciamos una serie de demandas en conjunto con Pfizer porque también había mucho *Spam* de viagra, y ese viagra es pirata entonces el procurador del Estado de Nueva York, Pfizer y nosotros estamos combatiendo ese *Spam*, es típico ese *Spam* de viagra.

Entonces estamos coadyuvando iniciativa privada y gobierno para tratar de atacarlo, entonces nosotros lo atacaremos solamente en la medida que tengamos un marco regulatorio por eso el estudio de hoy es muy interesante porque dicen si es que México no pues no hay Spammers, puede ser cierto ahorita pero si tu si te sabes los diez mandamientos del Hacker: su primera es conoce la legislación del país donde estas operando, es su primer regla y la saben, y la conocen mucho mejor que nosotros, fíjate en Julio México generó dos mil seiscientos millones de correo basura, México ya lo generó, en envío de publicidad de medicamentos ya ocupa el 41% y ocupa mensajes en contenido para adultos o sea actividades delictivas el 10% y es el 72% en correo mundial, entonces ya dos mil millones de correo están saliendo de México, entonces si no queremos ser el paraíso para los Spammers necesitamos tener una legislación adecuada.

SL: Sobretodo todo es bueno lo que hace Microsoft en cuanto a los casos en especial en Estados Unidos donde se está generando mas el *Spam* ,es una imagen de lo que se puede hacer a nivel mundial imponer sanciones económicas muy altas.

MD: No y no solamente es económica, la razón por la cual estamos llegando a acuerdos es porque realmente es la pérdida de su libertad o sea es un delito que tiene una pena corporal, a cambio de esa pena corporal estamos logrando negociar arreglos económicos. Pero la pena es corporal y es un problema mundial y requiere de resultados mundiales o sea nosotros tenemos acciones de antispam en Australia, Europa, Japón es las legislaciones que ya tienen legislación y lo apoya mientras no.

SL: Le agradezco su apoyo al concederme esta entrevista para mi proyecto de investigación.