

**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**

**AUSENCIA DE LEGISLACIÓN QUE PROTEJA EL DERECHO DE INTIMIDAD Y
PRIVACIDAD DE LAS PERSONAS INDIVIDUALES Y JURÍDICAS EN GUATEMALA
CONTRA EL ENVÍO DE CORREOS ELECTRÓNICOS NO SOLICITADOS O NO
DESEADOS**

JOSÉ AUGUSTO BOLAÑOS JIMÉNEZ

GUATEMALA, NOVIEMBRE DE 2009

**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**

**AUSENCIA DE LEGISLACIÓN QUE PROTEJA EL DERECHO DE INTIMIDAD Y
PRIVACIDAD DE LAS PERSONAS INDIVIDUALES Y JURÍDICAS EN GUATEMALA
CONTRA EL ENVÍO DE CORREOS ELECTRÓNICOS NO SOLICITADOS O NO
DESEADOS**

TESIS

Presentada a la Honorable Junta Directiva
de la
Facultad de Ciencias Jurídicas y Sociales
de la
Universidad de San Carlos de Guatemala

Por

JOSÉ AUGUSTO BOLAÑOS JIMÉNEZ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

Y los títulos profesionales de

ABOGADO Y NOTARIO

Guatemala, noviembre de 2009.



**HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**

DECANO: Lic. Bonerge Amilcar Mejía Orellana
VOCAL I: Lic. César Landelino Franco López
VOCAL II: Lic. Gustavo Bonilla
VOCAL III: Lic. Erick Rolando Huitz Enríquez
VOCAL IV: Br. Marco Vinicio Villatoro López
VOCAL V: Br. Gabriela María Santizo Maldonado
SECRETARIO: Lic. Avidán Ortiz Orellana

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera Fase:

Presidente: Lic. Gerardo Prado
Vocal: Licda. Lilian Consuelo Montes Mendoza
Secretaria: Licda. Patricia Gonzalez de Sentes

Segunda Fase:

Presidente: Lic. Ricardo Alvarado Sandoval
Vocal: Lic. Ronaldo Amilcar Sandoval
Secretaria: Licda. Eloisa Mazariegos Herrera

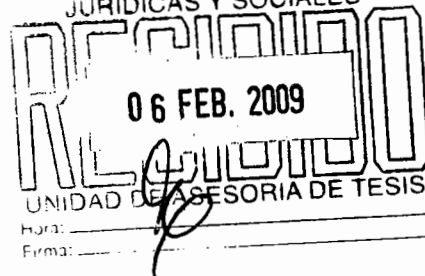
RAZÓN: “Únicamente el autor es responsable de las doctrinas sustentadas y contenido de la tesis”. (Artículo 43 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).



**LICDA. IRMA ILEANA ESCOBAR Y ESCOBAR
ABOGADA Y NOTARIA**

9ª. Avenida 7-35, zona 1 Segundo Nivel, Of. 233 Edificio Galerías Plaza Central
Teléfono 2232-5196

Guatemala, 30 de octubre de 2008
FACULTAD DE CIENCIAS
JURIDICAS Y SOCIALES



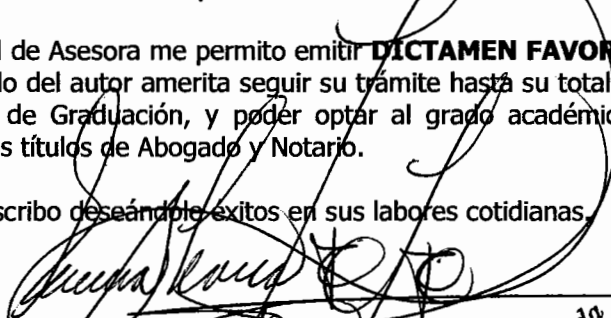
**Licenciado
Carlos Castro Monroy
Jefe de la Unidad de la Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala.
Su Despacho.**

Honorable Licenciado Castro Monroy:

En cumplimiento al nombramiento recaído en mi persona, en mi calidad de Asesora del trabajo de tesis del Bachiller **JOSÉ AUGUSTO BOLAÑOS JIMÉNEZ**, intitulado **"AUSENCIA DE LEGISLACIÓN QUE PROTEJA EL DERECHO DE INTIMIDAD Y PRIVACIDAD DE LAS PERSONAS INDIVIDUALES Y JURÍDICAS EN GUATEMALA CONTRA EL ENVÍO DE CORREOS ELECTRÓNICOS NO SOLICITADOS O NO DESEADOS"**, resulta procedente dictaminar respecto a la asesoría del mismo de conformidad con las siguientes justificaciones:

- 1.- El contenido objeto de desarrollo, análisis, aportaciones y teorías sustentadas por estudiante José Augusto Bolaños Jiménez, ameritó ser calificado de sustento importante y valedero al momento de la asesoría efectuada; circunstancia académica que desde todo punto de vista deben concurrir y son atinentes a un trabajo de investigación de tesis de grado.
- 2.- Aunado a lo expuesto se pudo establecer que el referido trabajo de investigación se efectuó apegado a la asesoría prestada, habiéndose apreciado el cumplimiento a los presupuestos tanto de forma como de fondo, exigidos por el Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público de la Facultad de Ciencias Jurídicas y Sociales, de nuestra Universidad Rectora de la Educación Superior, en el presente dictamen se determina expresamente que el trabajo de investigación cumple satisfactoriamente con los requisitos establecidos en el Artículo treinta y dos (32) de dicho normativo, ya que se pudo verificar su contenido científico y técnico en la elaboración del tema, su técnica así como su método de investigación fueron los indicados. Las conclusiones y las recomendaciones están buscando el verdadero objeto del tema como lo es contribuir a resolver el problema social objeto de su trabajo; carece de cuadros estadísticos ya que no fue necesario y por último pude constatar que la bibliografía era la adecuada para la elaboración del tema.
- 3.- En consecuencia en mi calidad de Asesora me permito emitir **DICTAMEN FAVORABLE**, en el sentido de que el trabajo de tesis de grado del autor amerita seguir su trámite hasta su total aprobación para ser discutido en su Examen Público de Graduación, y poder optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales y a los títulos de Abogado y Notario.

Sin otro particular, me suscribo deseándole éxitos en sus labores cotidianas.


Licda. Irma Ileana Escobar Y Escobar
Abogada y Notaria
Asesora, Colegiado 7271

*Licenciada
Irma Ileana Escobar Y Escobar
Abogada y Notaria*



UNIDAD ASESORÍA DE TESIS DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES. Guatemala, nueve de febrero de dos mil nueve.

Atentamente, pase al (a la) **LICENCIADO (A) NAPOLEÓN GILBERTO OROZCO MONZÓN**, para que proceda a revisar el trabajo de tesis del (de la) estudiante **JOSÉ AUGUSTO BOLAÑOS JIMÉNEZ**, Intitulado: **“AUSENCIA DE LEGISLACIÓN QUE PROTEJA EL DERECHO DE INTIMIDAD Y PRIVACIDAD DE LAS PERSONAS INDIVIDUALES Y JURÍDICAS EN GUATEMALA CONTRA EL ENVÍO DE CORREOS ELECTRÓNICOS NO SOLICITADOS O NO DESEADOS”**.

Me permito hacer de su conocimiento que está facultado (a) para realizar las modificaciones de forma y fondo que tengan por objeto mejorar la investigación, asimismo, del título de trabajo de tesis. En el dictamen correspondiente debe hacer constar el contenido del Artículo 32 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, el cual dice: “Tanto el asesor como el revisor de tesis, harán constar en los dictámenes correspondientes, su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, las conclusiones, las recomendaciones y la bibliografía utilizada, si aprueban o desaprueban el trabajo de investigación y otras consideraciones que estimen pertinentes”.


LIC. CARLOS MANUEL CASTRO MONROY
JEFE DE LA UNIDAD ASESORÍA DE TESIS

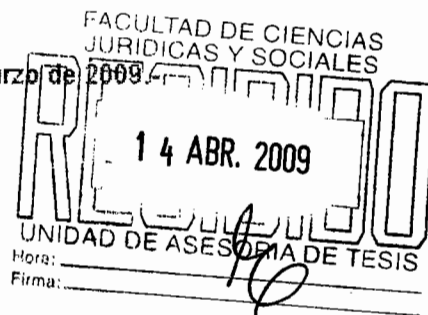


cc.Unidad de Tesis
CMCM/nnmr



LIC. NAPOLEÓN GILBERTO OROZCO MONZÓN
ABOGADO Y NOTARIO
5ª. Avenida 10-68 zona 1 Of.302 piso 3
Edif. Helvetia, Guatemala, C.A.
TEL.22324664

Guatemala, 02 de marzo de 2009



Licenciado Carlos Manuel Castro Monroy
Jefe de la Unidad de Asesoría de Tesis
De la Facultad de Ciencias Jurídicas y Sociales
De la Universidad de San Carlos de Guatemala
Su Despacho.

Licenciado:

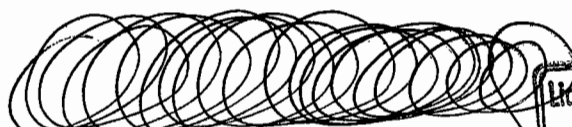
De la manera más atenta me permito comunicarle que he cumplido con la función de Revisor de Tesis del estudiante JOSÉ AUGUSTO BOLAÑOS JIMÉNEZ, intitulado "AUSENCIA DE LEGISLACIÓN QUE PROTEJA EL DERECHO DE INTIMIDAD Y PRIVACIDAD DE LAS PERSONAS INDIVIDUALES Y JURIDICAS EN GUATEMALA CONTRA EL ENVÍO DE CORREOS ELECTRÓNICOS NO SOLICITADOS O NO DESEADOS", el cual a mi criterio cumple con todos los requisitos y formalidades que establece la normativa de esta facultad, y emito el dictamen siguiente:

1. Considero que el tema investigado por el estudiante José Augusto Bolaños Jiménez, es de suma importancia respecto a su contenido científico y técnico, por lo que puede llegarse a la conclusión de que el mismo, no solo reúne los requisitos exigidos por la normativa correspondiente, sino además, se presenta con una temática de especial importancia para el Congreso de la República de Guatemala, tomará la decisión de dictar una legislación antispam. Y concluye que el spam es un problema considerable y creciente para los usuarios, las redes e Internet en general.

2. La bibliografía empleada por el estudiante Bolaños Jiménez, fue la adecuada al tema elaborado y sus conclusiones resultan congruentes con su contenido y las recomendaciones son consecuencia del análisis jurídico de la investigación realizada; habiendo empleado en su investigación los métodos históricos, deductivos e inductivo y con relación a las técnicas, ficheros, fichas de trabajo, etc.; haciendo aportaciones valiosas y propuestas concretas para su realización.

3. En definitiva, el contenido del trabajo de tesis, se ajusta a los requerimientos científicos y técnicos que se deben cumplir de conformidad con la normativa respectiva, la metodología y técnicas de investigación utilizadas, la redacción, las conclusiones y recomendaciones, bibliografía utilizada son congruentes con los temas desarrollados dentro de la investigación, es por ello que al haberse cumplido con los requisitos establecidos en el Artículo 32 del Normativo para Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y Examen General Público, resulta procedente dar el presente DICTAMEN FAVORABLE, aprobando el trabajo de tesis considerando conveniente la impresión de mismo para que pueda ser discutido en el correspondiente examen público.

Sin más que agradecer la consideración a mi persona, al encomendarme tan honroso trabajo de Revisor, aprovecho la oportunidad para reiterarle mi alta muestra de estima. Sin otro particular, me suscribo muy cordialmente.-

F) 
LIC. NAPOLEÓN GILBERTO OROZCO MONZÓN
COL. 2661

Lic. Napoleón Gilberto Orozco Monzón
ABOGADO Y NOTARIO

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA



FACULTAD DE CIENCIAS
JURÍDICAS Y SOCIALES

Ciudad Universitaria, zona 12
Guatemala, C. A.

DECANATO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES.

Guatemala, veintiocho de agosto del año dos mil nueve.

Con vista en los dictámenes que anteceden, se autoriza la Impresión del trabajo de Tesis del (de la) estudiante JOSÉ AUGUSTO BOLAÑOS JIMÉNEZ, Titulado AUSENCIA DE LEGISLACIÓN QUE PROTEJA EL DERECHO DE INTIMIDAD Y PRIVACIDAD DE LAS PERSONAS INDIVIDUALES Y JURÍDICAS EN GUATEMALA CONTRA EL ENVÍO DE CORREOS ELECTRÓNICOS NO SOLICITADOS O NO DESEADOS. Artículos 31, 33 y 34 del Normativo para la elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.-

CMCM/sllh





DEDICATORIA

- A DIOS: Mi creador, sustentador, proveedor y salvador, fuente de sabiduría y quien en cumplimiento a su promesa, me ha acompañado en cada momento de mi vida hasta el día de hoy. Y a mis ángeles que me han protegido.
- A MI PATRIA: Lugar hermoso que me ha brindado abrigo y donde Dios me ha puesto para cumplimiento de su propósito.
- A MIS PADRES: César Augusto Bolaños Del Cid (Q.E.P.D.) y María del Rosario Jiménez Batres. Quienes han sido mi ejemplo, ayuda, apoyo y estímulo para finalizar lo que ellos iniciaron hace mucho tiempo, con esfuerzo y privaciones.
- A MIS HERMANOS: Yoli, Delia, Aurelia, Angélica, Julio y Tomás. Por la ayuda y apoyo incondicional brindado en todo momento.
- A MI FAMILIA
EN GENERAL: Porque han creído en la realización y culminación de mi carrera desde que ésta inició.
- A MIS AMIGOS
Y COMPAÑEROS: Fredy Morán, Pablo Retana, Nery Méndez, Bayron González, Julio César Enríquez, Luis Alfredo Hernández, Edvin López, Luis Silvestre, Esvin Soto, y muchos más a los que no menciono, pero saben quienes son. Por su paciencia y ayuda a lo largo de estos años de estudio.



A LA UNIVERSIDAD DE
DE SAN CARLOS DE
GUATEMALA:

Por brindarme la oportunidad de pertenecer a esta casa de estudios y realizar mi formación académica; especialmente a la Facultad de Ciencias Jurídicas y Sociales.



ÍNDICE

Pág.

Introducción.....	i
-------------------	---

CAPÍTULO I

1. Correo electrónico no deseado, spam.....	1
1.1. Antecedentes históricos.....	1
1.2. Generalidades.....	5
1.3. Formas y tipos de spam	10
1.4. Glosario de términos de spam.....	13

CAPÍTULO II

2. Spam y su relación con los derechos de privacidad e intimidad.....	17
2.1. Generalidades del derecho a la intimidad.....	17
2.2. Generalidades del derecho a la privacidad.....	20
2.3. Análisis del fundamento legal guatemalteco de los derechos a la intimidad y a la privacidad.....	22
2.4. Relación actual de los derechos a la intimidad y privacidad en contraposición al correo electrónico no deseado o no solicitado.....	24
2.5. Lineamientos para prevenir el correo electrónico no deseado o no solicitado.....	27
2.6. Lineamientos para reducir el correo electrónico no deseado o no solicitado.....	30

CAPÍTULO III

3. Se debe legislar a favor de garantizar los derechos a la intimidad y privacidad en el contexto legal guatemalteco, con relación al spam o correo electrónico no deseado.....	33
3.1. Análisis jurídico económico del abuso de direcciones de correo electrónico con fines publicitarios.....	33
3.2. Fundamentos y puntos para legislar contra el envío de correos electrónicos no deseados o no solicitados, spam.....	42

3.3. Legislación vigente a nivel nacional enfocada a los correos electrónicos no deseados o no solicitados, spam.....	45
3.4. Legislación vigente a nivel internacional enfocada a los correos electrónicos no deseados o no solicitados, spam.....	47
3.5. Análisis de caso concreto sobre sentencia en control del spam en la legislación colombiana.....	60
3.6. Decálogo para prevenir y sancionar el spam, aprobado por la Agencia Española de Protección de Datos.....	80

CAPÍTULO IV

4. Propuesta de proyecto de Ley anti spam en Guatemala.....	83
4.1. Propuesta sobre aspectos que debe contener un proyecto anti spam en nuestro país.....	83
4.2. Criterios para calificar el correo comercial no solicitado.....	91
4.3. Criterios para calificar el correo ilegal no solicitado.....	92
4.4. Derechos y obligaciones del usuario y proveedor de servicios de internet	93
 CONCLUSIONES.....	 95
RECOMENDACIONES.....	97
BIBLIOGRAFÍA.....	99



INTRODUCCIÓN

El tema elegido que se presenta a continuación, surge directamente de una inquietud personal del suscrito, a pesar de comentarios o posturas de personas que lo catalogan como no importante o de poca trascendencia para nuestra legislación nacional, inclusive en momentos de pensamientos propios de carácter negativo. Pero cabe destacar, que la motivación a desarrollarlo, toma fuerza interior al comenzar a investigar sobre el mismo, dentro de la cual se encontraron fundamentos de peso como para poder presentarlo como un trabajo válido y de actualidad, que vino a reforzar el deseo de compartir esta inquietud con compañeros estudiantes y profesionales del derecho, sobre lo que realmente sucede en este nuevo siglo, en esta nueva época llamada o conocida internacionalmente como una sociedad de la información, en donde Guatemala y, específicamente esta facultad, no pueden quedar ajenas a los nuevos acontecimientos y situaciones que actualmente preocupan a los Estados y que, por ende, tratan de encuadrarlos en normas jurídicas eficientes, que tiendan a regularizar las nuevas conductas en las que el hombre está incurriendo, debido a la nueva forma de sociedad que se vive en estos tiempos.

Dentro de los objetivos planteados al realizar esta investigación, se pueden mencionar como principales, el poder fundamentar la necesidad de una legislación en el ordenamiento jurídico guatemalteco, que permita garantizar efectivamente la seguridad de los datos personales, como lo es la dirección de correo electrónico, utilizado por personas individuales o jurídicas, señalando la problemática actual acerca del abuso del uso del correo electrónico, y su incidencia en el ámbito empresarial y social; analizando desde la perspectiva jurídica, el envío de correos electrónicos no deseados o no solicitados en el medio internacional y nacional, para poder llegar a proponer un estudio actualizado y avanzado del tema propuesto, tanto para estudiantes como para los ya profesionales del derecho, incluido un proyecto ley de cómo debería legislarse en esta materia, tomando en cuenta las normas del derecho comparado ya existente. La hipótesis está relacionada a una propuesta para regular a favor de garantizar efectivamente el derecho a la intimidad y privacidad de



los ciudadanos guatemaltecos contra el envío desmedido y abusivo de correos electrónicos no solicitados o no deseados.

El presente trabajo de investigación está dividido en cuatro capítulos: el capítulo I que trata acerca de conceptos básicos acerca del correo electrónico no deseado, spam; el capítulo II se refiere al spam y su relación con los derechos de privacidad e intimidad; el capítulo III hace referencia al deber de legislar a favor de garantizar los derechos a la intimidad y privacidad en el contexto guatemalteco, con relación al spam o correo electrónico no deseado y; el capítulo IV en el cual se incluye una propuesta de proyecto de Ley anti spam en Guatemala; capítulos que fueron desarrollados con la convicción de crear en el lector el interés por el análisis y comprensión de cada uno de los temas tratados.

Una de las prácticas más aparejadas al internet es el uso y envío de correos electrónicos o e-mails; herramienta que proporciona una comunicación rápida, efectiva y en tiempo casi real; es decir, se recibe la correspondencia inmediatamente en cuestión de minutos, y no hay necesidad de esperar a que el correo tradicional entregue lo que se quiere comunicar a través de un documento o carta, por ejemplo en uno o varios días, sino que a través de utilizar el servicio de internet y, a su vez, la aplicación de un correo electrónico; en cuestión de minutos se puede acceder a esta información, acortando distancias y comunicando a las personas efectivamente.

Pero, como suele suceder con todas las aportaciones que significan un desarrollo social, de la mano a ese avance, comienzan a surgir prácticas contrarias al objetivo para lo cual fueron creadas, tal es el caso del mal uso que actualmente se le está dando a las direcciones de correos electrónicos, ya que a diario los usuarios de la red internet reciben correos que no han sido solicitados y que son enviados por desconocidos con distintos fines, conocido en el ámbito internacional como spam; y que dentro del desarrollo de este trabajo se verán las grandes implicaciones que conlleva este nuevo problema y la ausencia de legislación que lo regule.



CAPÍTULO I

1. Correo electrónico no deseado spam

1.1. Antecedentes históricos

El origen de la palabra spam tiene raíces estadounidenses ya que la empresa de embutidos estadounidense denominada Hormel Foods lanzó en 1937 una carne en lata originalmente llamada Hormel's Spiced Ham. El gran éxito del invento lo convirtió con el tiempo en una marca genérica, tan conocida que hasta el mismo fabricante le recortó el nombre, dejándolo con solo cuatro letras: spam. Este nuevo tipo de alimento enlatado, alimentó a los soldados soviéticos y británicos en la Segunda Guerra Mundial, y desde 1957 fue comercializado en todo el mundo. En los años 60 se hizo aún más popular gracias a su innovador anillo de apertura automática, que ahorraba al consumidor el uso del abrelatas y le evitaba molestias.

Fue entonces cuando los **Monty Python** (personajes de la televisión británica) empezaron a hacer burla de la carne en lata. Su divertidísima costumbre de gritar la palabra *spam* en diversos tonos y volúmenes se trasladó metafóricamente al correo electrónico no solicitado, que perturba la comunicación normal en internet.

En un famoso corto televisivo de 1970 (Flying Circus) los personajes de televisión británica representaban a un grupo de hambrientos vikingos atendidos por hermosas meseras que les ofrecían "huevo y tocino; huevo, salchichas y tocino; huevo y spam; huevo, tocino, salchichas y spam; spam, tocino, salchichas y spam; spam, huevo, spam, spam, tocino y spam; salchichas, spam, spam, tocino, spam, tomate y spam, ...". La escena acababa con los vikingos cantando a coro "spam, spam, spam, spam. ¡Rico spam! ¡Maravilloso spam! spam, spa-a-a-a-am, spa-a-a-a-a-am, spam. ¡Rico spam! ¡Rico spam! ¡Rico spam! ¡Rico spam! spam, spam, spam, spam".

Como la canción, el spam resulta ser una repetición sin fin de texto de muy poco valor o ninguno, que aplicado a los mensajes electrónicos, se refiere a los mensajes enviados

de forma masiva y dirigidos a personas que, en principio o de primera intención, no desean recibirlos.

Esta practica se ha vuelto tan común que ahora la mayor parte de los mensajes (más del 40%) proceden de Estados Unidos (a pesar de que allí está prohibido), seguido por Corea del Sur (15%) y China (12%).

Podemos decir, que spam es una palabra inglesa que hace referencia a una conserva cárnica: el "Spiced Ham", literalmente "Jamón con especias". Al no necesitar refrigeración, fue muy utilizada en todo el mundo, sobre todo por el ejército americano, que ayudó mucho en su difusión. Debido a esto (y a su baja calidad) se ha utilizado este término para hacer referencia a todos los mensajes basura que se reciben tanto en los grupos de noticias como en los buzones particulares.

El correo basura mediante el servicio de correo electrónico podría decirse que nació como tal el 5 de marzo de 1994, ya que ese día un bufete de abogados estadounidense llamada de *Canter and Siegel*, publica en Usenet (servicio de red) un mensaje de anuncio de su firma legal, el cual en el primer día después de la publicación, facturó cerca de 10.000 dólares por casos de sus amigos y lectores de la red. Desde ese entonces, el marketing mediante correo electrónico ha crecido a niveles impensados desde su creación.

Con la evolución reciente de este nuevo fenómeno conocido como spam (correos electrónicos no solicitados y no deseados) podemos distinguir tres etapas, visualizadas de manera mejor con tres casos que las marcaron, a saber:

A) La primera etapa corresponde al primer caso de spam ampliamente publicitado, el de dos abogados de Arizona, Estados Unidos de Norte América, de nombres Laurence Canter y Martha Siegel quienes se dedicaron a promover sus servicios utilizando grupos de discusión Usenet durante 1994. Laurence Canter y Martha Siegel eran una pareja de abogados que un día de 1993 comenzaron a ofrecer servicios legales relacionados con asesoría en materias de inmigración que consistían en asegurar a sus potenciales clientes –previo pago de US \$100- su inclusión en las listas



de lotería que seleccionan las solicitudes de visa que serán tramitadas. La oferta de la firma de abogados fue llevada a cabo poniendo un aviso en más de 6.000 grupos de discusión Usenet. La pequeña firma de abogados recibió un buen número de respuestas de clientes potenciales. Junto a esto, recibieron miles de respuestas airadas reclamando el envío de publicidad no solicitada. Esta avalancha de respuestas excedió la capacidad del proveedor de servicios de internet de los abogados, de manera que, al corto andar, su cuenta fue cancelada. Algo más tarde, la pareja de abogados publicó un libro llamado Cómo hacer fortuna en la superautopista de la información (how to make a fortune on the information superhighway) en el cual presentaban técnicas de recolección de direcciones de correo electrónico desde grupos de discusión (en internet) y sobre cómo enviar masivamente publicidad por medios electrónicos.

B) La segunda etapa queda bien ilustrada a través de la obstinada gestión de Jeff Slaton, conocido como el “Rey del spam.” Jeff fue uno de los lectores del libro de los abogados Canter y Siegel, quien para esa época era el representante de Yellow Pages (Páginas Amarillas) en Albuquerque, quien se dedicó a enviar avisos a grupos de discusión ofreciendo los planos de la bomba atómica por US \$18. Slaton descubrió que el negocio prosperaba y cambió su modelo de negocios desde el envío de publicidad hacia la venta de campañas publicitarias realizadas a través del envío de spam. De esta manera Slaton se transformó en el primero en ofrecer sus servicios como “spammer”, autoproclamándose el rey del spam. Junto a esto inauguró algunas técnicas actualmente comunes en el envío de publicidad masiva en plataformas electrónicas como direcciones falsas de correo electrónico en el caso del emisor y nombres de dominio falsos para evitar la detección y desviar las quejas, por lo que de esta forma el señor Jeff Slaton inauguró las empresas dedicadas al spam.

C) Finalmente, la última etapa corresponde a lo gestionado por Sanford Wallace en Cyber Promotions, quien en 1996, Sanford Wallace (quien luego sería conocido como “Spamford”) dueño de Cyber Promotions, una compañía con sede en Philadelphia, Estados Unidos de Norte América, comenzó a enviar publicidad no

solicitada a los correos electrónicos provistos por AOL19, llegando, en su punto más álgido, al envío de 30 millones de correos diarios. American On Line AOL (sistema de navegación en internet) respondió a esto bloqueando las direcciones desde donde Wallace enviaba sus correos. En respuesta Wallace demandó a AOL por infringir el derecho a la libertad de expresión consagrado en la Primera Enmienda de la Constitución de los Estados Unidos. Una semana antes que la demanda de Wallace fuera desestimada, este compareció una vez más ante los tribunales, pero esta vez como demandado. Los demandantes eran tres proveedores de servicios en línea de nombres Compuserve, Prodigy y Concentric Networks alegando que Caber Promotions estaba utilizando sus nombres de dominio para evitar los filtros instalados por AOL para prevenir el ingreso de correos electrónicos enviados por Cyber Promotions. *Spamware y proveedores de servicios de spam.*

Actualmente quienes se dedican a enviar spam o correos electrónicos no deseados, utilizan dos tipos de herramientas, las primeras sirven para recolectar direcciones de correo electrónico y las segundas para enviar las comunicaciones electrónicas masivas no deseadas. A estas dos herramientas en conjunto se les denomina “spamware”.

Las herramientas de recolección, permiten recolectar direcciones de correo electrónico de la Red y de grupos de discusión. Aún cuando existen listas de correos electrónicos disponibles para la venta, la ventaja de las herramientas de recolección es que evitan el número de direcciones duplicadas de correos electrónicos que suelen contener las listas de usuarios. El segundo riesgo que se evita al no optar por listas es que quienes figuren en dichas listas ya hayan sido víctimas de numerosas campañas de spam y posean sistemas de filtro y bloqueo. Las herramientas de recolección son sencillas de utilizar y permiten al usuario clasificar las direcciones que pretende recolectar. Con todo esto, algunas de estas herramientas poseen la capacidad de rescatar información simultáneamente desde varios sitios y luego filtrarla eliminando aquellas direcciones que se repiten.

Por otro lado las herramientas de envío presentan dos ventajas. Por una parte permiten al spammer enviar cantidades masivas de correo sin que esto lesione al proveedor de servicios de internet que el spammer está utilizando. Por otra, permiten eludir algunos de los filtros que utilizan los usuarios o los operadores de destino para evitar correos no deseados.

Concluyendo, los proveedores de servicios de spam en la actualidad, pueden agruparse en dos actividades principales: las de realización de campañas de spam y la creación de listas. En el primer rubro, el servicio ofrecido es la recolección, el envío de los mensajes y todos aquellos servicios que resulten necesarios para llevar adelante una campaña de publicidad a través de correos electrónicos masivos. En el segundo caso, creación de listas el servicio ofrecido es la venta de listas de direcciones de correos electrónicos, (muchas veces tomadas de forma ilegal, pues muchos poseedores de esas direcciones electrónicas no han expresado su consentimiento para tal fin.)

1.2. Generalidades

Actualmente se denomina spam o “correo basura” a todo tipo de comunicación **no solicitada o no deseada**, que se realiza por vía electrónica. Es decir, se entiende por spam cualquier mensaje no solicitado o no deseado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Esta practica se puede hacer por distintas vías siendo la más utilizada entre el público en general la herramienta del correo electrónico.

El correo basura (en inglés también conocido como *junk-mail* o *spam*) es una forma de inundar la internet con muchas copias (incluso millones) del mismo mensaje, en un intento por llegar a más personas que de otra forma nunca accedería a recibirlo y menos a leerlo. La mayor parte del correo basura está constituido por anuncios comerciales, normalmente de productos dudosos, métodos para hacerse rico o servicios en la frontera de la legalidad. No deja de amargar la existencia a los usuarios

de internet cuando encuentran sus buzones llenos de correos del estilo como: “Gane millones trabajando desde casa”, “Dieta milagrosa — pierda 10 kilos en una semana” “Chicas XXX sensuales te están esperando”, por mencionar algunos ejemplos. Las listas de correo basura con las direcciones de correo electrónico de los clientes potenciales (o víctimas seguras) se crean frecuentemente de los mensajes de Usenet (salas de discusión), robando direcciones en las listas de distribución o comprándolas en las bases de datos de los servicios en línea de internet o bien buscando direcciones por la red.

Se puede enfocar que el problema del spam o envío de correos electrónicos no deseados o no solicitados, radica potencialmente desde el punto de vista del costo financiero con el que cargan los navegantes de la internet, ya que por ejemplo un usuario europeo promedio de Internet que paga una tarifa plana de € 12 mensual por diez horas de conexión (incluyendo las llamadas de teléfono) y usando equipo estándar (sin banda ancha) puede bajar mensajes a una velocidad de aproximadamente 180 K/bits por minuto, el costo de bajar alrededor de 15 mensajes al día sumando entre 500 y 800 K/bits en tamaño puede costar tanto como €30 al año. Si esta cantidad es multiplicada por el número de usuarios de internet en un país el costo total llega a ser muy sustantivo. Llevando esto a escala planetaria, asumiendo una comunidad mundial de 400.000 de usuarios, el costo global de bajar mensajes de aviso utilizando la tecnología actual podría ser estimado conservadoramente en €10 mil millones —y esta es solo una porción de los costos soportados directamente por los Navegantes

Básicamente, podemos afirmar que las definiciones más aceptadas o utilizadas de spam son: a) correos electrónicos comerciales no solicitados y b) correos electrónicos masivos no solicitados. Lo que resulta común en ambos casos es que se trata de correo electrónico no solicitado. Y en general se ha entendido por *no solicitado* un correo en aquellos casos en que: no existe relación previa entre las partes y el receptor no ha consentido explícitamente en recibir la comunicación, también incluye que el receptor previamente ha buscado terminar una relación existente, usualmente instruyendo a la otra parte de no enviarle más comunicaciones en el futuro; y lo que, en

principio, califica al correo no solicitado como spam es su característica comercial, la cantidad enviada o una combinación de de ambos.

Aún cuando la definición de *comercial* varía en las distintas legislaciones, lo que suele considerarse en el caso de las comunicaciones comerciales es la promoción de algún tipo de bienes o servicios. En este sentido, por ejemplo, la Directiva 2000/31 de las Comunidades Europeas define en su Artículo 2 literal f) comunicaciones comerciales como: “todas las formas de comunicación destinadas a proporcionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización con una actividad comercial, industrial o de profesiones reguladas...”

Con respecto al carácter *masivo* se plantean dos interrogantes, al momento de legislar en relación al spam. La primera es si debe tratarse del mismo mensaje enviado en forma multitudinaria para que sea tomado como spam o puede tratarse de mensajes substancialmente similares. La segunda es cuántos mensajes deben enviarse para que dicho envío sea considerado masivo. La principal pregunta a este respecto es si debiese fijarse un umbral –por ejemplo, 1000 correos electrónicos- o dejar la norma abierta. Con lo anotado no se pretende enredar en cuanto a la definición correcta sobre el spam, sino manifestar que en la actualidad aún no se tiene generalizada dicha definición ya que se cuentan con estas dificultades por lo que la legislación varía con los avances tecnológicos, con el objeto de presentar una legislación no solo vigente sino positiva.

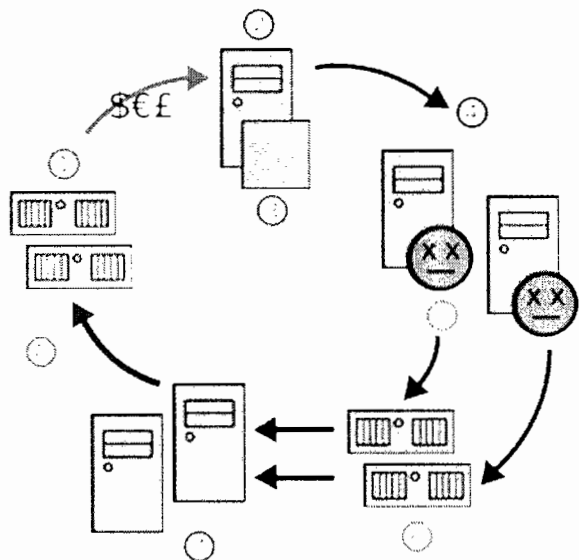
Actualmente, el correo electrónico es, el medio más común de *spamming* en internet, lo cual significa enviar mensajes idénticos o casi idénticos a un gran número de direcciones. A diferencia de los correos electrónicos comerciales legítimos, el spam generalmente es enviado sin el permiso explícito de los receptores, y frecuentemente contiene varios trucos para sortear los filtros de verificación de correos legítimos. Las computadoras modernas generalmente vienen con cierta capacidad para enviar spam. El único ingrediente necesario es la lista de direcciones objetivo. El receptor de spam puede verse perjudicado al tener que invertir tiempo en eliminar mensajes de su cuenta



de correo electrónico; sin embargo, diferentes sistemas de correo en línea (como Windows Live, Yahoo! y Gmail) han incrementado sustancialmente la capacidad de almacenamiento de las respectivas cuentas (Yahoo! Es un correo que actualmente tiene una capacidad de almacenamiento ilimitada). Por otro lado, la recepción de estos correos no deseados, genera una utilización del ancho de banda de acceso a internet sin ninguna necesidad por parte del usuario, que es quien paga por el servicio.

El bajo costo de los envíos vía internet (mediante el correo electrónico) o mediante telefonía móvil (SMS y MMS), su posible anonimato, la velocidad con que llega a los destinatarios y las posibilidades en el volumen de las transmisiones, han permitido que esta práctica se realice de forma abusiva e indiscriminada.

Esta conducta, es particularmente grave cuando se realiza en forma masiva y con esta base, el envío de mensajes comerciales sin el consentimiento previo está prohibido legalmente en varios países de mundo, como por ejemplo por la legislación española, tanto por la Ley 34/2002 de Servicios de la Sociedad de la Información (a consecuencia de la transposición de la Directiva 31/2000/CE) como por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos. Para un ejemplo específico, podemos decir, que la ley española, de Servicios de la Sociedad de la Información, en su Artículo 21.1 prohíbe de forma expresa el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. Es decir, están prohibidas todas las comunicaciones dirigidas a la promoción directa o indirecta de los bienes y servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, si bien esta prohibición encuentra la excepción en el segundo párrafo del artículo, que autoriza el envío cuando exista una relación contractual previa y se refiera a productos similares. Para tener una mejor visualización y comprensión de cómo se desarrolla el spam o los correos electrónicos no deseados o no solicitados, presentamos el siguiente esquema:



Ciclo del SPAM

- (1): Sitio web de Spammers
- (2): Spammer
- (3): Spamware
- (4): ordenadores infectados
- (5): Virus o troyanos
- (6): Servidores de correo
- (7): Usuarios
- (8): Tráfico Web

1.3. Formas y tipos de spam

Como hemos mencionado el spam, ingresa de manera muy silenciosa a miles de hogares y empresas a través del correo electrónico, en la actualidad se perfila como uno de los principales problemas de internet y todavía no existe ninguna medida completamente efectiva que permita evitar, al cien por ciento esta mala práctica.

Existen varias formas en las que se pueden enviar los mensajes no deseados o no solicitados, así como diversos tipos de los mismos, entre lo que mencionamos:

a) Formas de spam: se pueden enviar mensajes no deseados a través de:

- Correos electrónicos:

Debido que presenta mayor facilidad, rapidez y capacidad en las transmisiones de datos, la recepción de comunicaciones comerciales a través de este servicio de la sociedad de la información es la más usual, y el medio por el que los *spammers* envían más publicidad no deseada.

- Spam por ventanas emergentes (Pop ups):

Se trata de enviar un mensaje no solicitado que emerge cuando nos conectamos a internet. Aparece en forma de una ventana de diálogo y advertencia del sistema Windows titulado "servicio de visualización de los mensajes". Su contenido es variable, pero generalmente se trata de un mensaje de carácter publicitario. Para ello se utiliza una funcionalidad del sistema de explotación Windows, disponible sobre las versiones Windows NT4, 2000, y XP y que permite a un administrador de redes enviar mensajes a otros puestos de la red.

- Phising:

No es exactamente una modalidad de spam, más bien una técnica de ingeniería social para recolectar datos de forma fraudulenta. El *Phising* es la duplicación de una página web para hacer creer al visitante que se encuentra en la página original en lugar de en la ilícita. Se suele utilizar con fines delictivos duplicando páginas de internet de bancos y enviando indiscriminadamente correos mediante spam para que se acceda a esta página con el fin de actualizar los datos de acceso al banco, como contraseñas, fechas de caducidad, etc.

- Hoax:

El *hoax* es un mensaje de correo electrónico con contenido falso o engañoso y normalmente distribuido en cadena. Algunos *hoax* informan sobre virus, otros invocan a la solidaridad, o contienen fórmulas para ganar millones o crean cadenas de la suerte. Los objetivos que persigue quien inicia un *hoax* son normalmente captar direcciones de correo o saturar la red o los servidores de correo.

- Scam:

El *Scam* no tiene carácter de comunicación comercial. Este tipo de comunicación no deseada implica un fraude por medios telemáticos, por vía teléfono móvil o por correo electrónico.

- Spam en el teléfono celular:

Además de las comunicaciones del operador de telefonía mediante mensajes de texto (SMS- *Short Message Services*), o mensajes multimedia (MMS- *Multimedia Message Services*), existen otro tipo de comunicaciones publicitarias en las que no media un consentimiento previo ni una relación contractual, por lo que son consideradas comunicaciones comerciales no solicitadas. Este tipo de comunicaciones generan un

gasto de tiempo y de dinero. Además los MMS pueden introducir virus y explotar de forma maliciosa alguna vulnerabilidad de los sistemas internos del teléfono.

b) Tipos de spam

Debido a la repercusión que conlleva el spam o los correos electrónicos no deseados, los podemos clasificar en:

- **Spam turístico:** también denominado estacional, consiste en falsas ofertas relacionadas con viajes y estancias hoteleras del estilo "le ha tocado un viaje al Caribe", clubs de vacaciones, etc.
- **Spam farmacéutico:** constituye uno de los grandes problemas del spam internacional, cada día millones de e-mails no solicitados llegan con anuncios de Viagra, Cialis, medicamentos y soluciones milagro, pérdida de peso, etc.
- **Spam rompecadenas:** se basa en enviar mensajes con rumores, leyendas urbanas, chistes u otras historias, el usuario las reenvía a amigos y/o familiares, sin saberlo está colaborando en una cadena de propagación que intenta captar el mayor número de e-mails para aumentar su base de datos.
- **Spam desinformativo:** responde a estrategias definidas por personas u organizaciones que intentan propagar un rumor o falsa información en Internet, a menudo lobbies cibernéticos.
- **Spam plagiarismo:** este tipo de correo no solicitado intenta vender software ilegal, libros, contenidos editoriales, música, películas a menudo copiadas sin pagar los correspondientes derechos de autor.

- **Spam erótico-pornográfico:** publicidad y mensajes de temática sexual, falsos mensajes procedentes de vinculadores de oferta y demanda sentimental, suscripciones a sitios web pornográficos, etc.

1.4. Glosario de términos de spam

Para mayor comprensión de los términos utilizados en el presente trabajo y a manera de ampliar la información relacionada con el mismo, me permito presentar el siguiente glosario de términos utilizados más frecuentemente dentro del contexto de los correos electrónicos no deseados o no solicitados.

Acuse de recibo: un tipo de mensaje que se envía para indicar que un correo ha llegado a su destino sin errores. Un acuse de recibo puede también ser negativo, es decir, indicar que un bloque de datos no ha llegado a su destino.

Antivirus: programa de ordenador que permite detectar y eliminar virus informáticos.

Can-spam Act: Ley federal por la que se encuadra la práctica del *spamming* en Estados Unidos, de 16 de diciembre de 2003 que entró en vigor el 1 de enero 2004. Este texto prevé un mecanismo de derecho de oposición. Esta ley prohíbe explícitamente los mensajes engañosos (utilización de falsas direcciones de expedición o el hecho de camuflar la naturaleza del mensaje) y la publicidad falsa del contenido del mensaje.

Cookies: conjunto de datos que envía un servidor Web a cualquier navegador que le visita, con información sobre la utilización que se ha realizado, por parte de dicho navegador, de las páginas del servidor, en cuanto a dirección IP del navegador, dirección de las páginas visitadas, dirección de la página desde la que se accede, fecha, hora, etc. Esta información se almacena en un fichero en el ordenador del usuario para ser utilizada en una próxima visita a dicho servidor. Además, existen servidores que restringen la utilización de determinadas funcionalidades de sus

servicios o, incluso, deniegan el uso de los mismos si el usuario decide no aceptar la grabación o colocación de la cookie en su ordenador.

Cortafuegos: sistema de seguridad que permite controlar las comunicaciones entre redes informáticas. Instalado entre internet y una red local permite evitar en esta última accesos no autorizados, protegiendo con ello su información interna.

Dirección de correo electrónico o e-mail: serie de caracteres, numéricos o alfanuméricos, que identifican un determinado recurso de forma única y permiten acceder a él. La dirección de correo electrónico está considerada como dato personal, ya que puede permitir la identificación del usuario de la misma.

Filtros: permiten ordenar el correo entrante basándose en una serie de reglas definidas previamente.

Hoax: del inglés, engaño o bulo.

Https: versión segura del protocolo http. El sistema HTTPS usa un cifrado basado en las *Secure Socket Layers* (SSL) para crear un canal más apropiado para el tráfico de información personal que el protocolo HTTP. Se utiliza normalmente por entidades bancarias, tiendas *on line*, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas.

IRC: siglas de *internet Relay Chat*, protocolo de comunicaciones que permite participar en conversaciones virtuales en tiempo real (véase Sala de Chat).

ISP: proveedor de Servicios a internet.

Lista negra: mecanismo de control de identificación que permite diferenciar entre personas que pueden acceder a un determinado servicio de otros que, constanding en dicha lista, no pueden acceder.

Opt-in: sólo mediante la petición expresa del particular, se podrá enviar comunicaciones comerciales. Se prohíbe todo tipo de comunicación comercial no consentida. Este es el mecanismo adoptado por las últimas Directivas Europeas. La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, transpuesta a nuestro derecho interno por la Ley 32/2003 General de Telecomunicaciones.

Opt-out: permite el envío libre de este tipo de comunicaciones siempre que permita al destinatario del mismo solicitar la exclusión de la lista de envíos. Esta era la antigua tendencia europea con respecto a la prestación del consentimiento, tal y como se preveía en la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de sociedad de la información y en particular el comercio electrónico en el mercado interior. En Estados Unidos sigue siendo el sistema legislativo vigente.

Phishing: es la contracción de "*password harvesting fishing*" (cosecha y pesca de contraseñas).

Red: conjunto de máquinas conectadas para intercambiar información entre sí.

Sala de Chat: lugar virtual de la red, llamado también canal, donde los usuarios se reúnen para charlar con otros que se encuentran en la misma sala.

Spam: envió masivo de correos electrónicos no solicitados o no deseados, correos electrónicos que se reciben en una dirección o cuenta específica sin la autorización expresa del titular de dicha cuenta.

Spammer: la persona o compañía que realiza el envío de spam.

Spamming lists: listas comerciales. Listas de direcciones de correo para envío de publicidad de forma masiva.

Spoofing: suplantación de la identidad de un tercero. Aunque puede producirse en diferentes entornos uno de los más habituales en los que aparece con frecuencia es en el envío masivo de spam.

URL: se refiere a una cadena de caracteres con la cual se asigna dirección única a cada uno de los recursos de información disponibles en internet.

Virus informático: programa de ordenador que puede infectar otros programas o modificarlos para incluir una copia de sí mismo. Los virus se propagan con distintos objetivos, normalmente con finalidades fraudulentas y realizando daños en los equipos informáticos.

Web bug: también se denominan “micro espías” o “pulgas” y son imágenes transparentes dentro de una página web o dentro de un correo electrónico con un tamaño de 1x1 pixeles. Al igual que ocurre con las *cookies*, se utilizan para obtener información acerca de los lectores de esas páginas o los usuarios de los correos, tales como la dirección IP de su ordenador, el tipo y versión de navegador del internauta, el sistema operativo, idioma, cuanta gente ha leído el correo, etc.

CAPÍTULO II

2. Spam y su relación con los derechos de privacidad e intimidad

2.1. Generalidades del derecho a la intimidad

Desde sus inicios la humanidad ha vivido en sociedad con la finalidad de satisfacer sus necesidades. Las relaciones que han surgido de esta vida en sociedad han sido reguladas por la sociedad misma, con el objeto de proporcionarle estabilidad y armonía. Así han surgido normas y leyes que deben ser respetadas y cumplidas por los individuos que se desenvuelven en ella. La explicación al afán de la sociedad, (representada por el Estado), de regular todas las actividades del ser humano podríamos decir, que tendría su base en el pensamiento de Nicolás Maquiavelo que en su obra El Príncipe expresa: “los hombres son siempre malos de no ser que la necesidad los torne buenos”.

El término de intimidad, se refiere a un derecho constitucionalmente reconocido y protegido, es objeto de tutela en las diversas ramas del ordenamiento jurídico de los distintos países. Según el Diccionario de la Academia de la Lengua Española, es la zona espiritual y reservada de un grupo de personas; esta definición coincide con la llamada “doctrina de la autodeterminación informativa”, creada por el Tribunal Constitucional Alemán en un fallo del 15 de diciembre de 1983, donde se instituye que es titular de los datos personales la propia persona y debe ser requerido su consentimiento por parte de terceros que deseen almacenarlos, cederlos o publicarlos; el Diccionario Jurídico de Ossorio y Gallardo, define al derecho a la intimidad como el derecho que tienen las personas a que su vida íntima sea respetada, que nadie se entrometa en la existencia ajena.

El avance de este derecho no es reciente, ya que podemos remontarnos al año 1890 donde una publicación en el diario "Harvard Law Review" salvaguardaba la propiedad de cada individuo sobre la propia privacidad, como el derecho de estar solo (*to be let alone*); pero en el siglo XX, el derecho a la intimidad adquiere un predominio especial ya que actualmente cubre un cúmulo de relaciones que el individuo mantiene sobre otros y que deben ser preservados como de su reserva personal. El derecho a la intimidad es el derecho de toda persona a que se le respete en su vida privada y familiar, y a evitar injerencias arbitrarias en la zona espiritual íntima y reservada de una persona. El nuevo derecho a la intimidad posee una faz preventiva y una faz reparadora: preventiva por la facultad de conocer los datos personales que constan en registros automatizados, de exigir la rectificación, actualización y cancelación de la información; y reparadora por la posibilidad de resarcimiento de daños y perjuicios por parte de quien lo padece.

La intimidad se afirma que un derecho entonces, personalísimo, según inspiración constitucional relativa a la dignidad humana, que debe ser tutelado cuando, por la acción de terceros, se produce una intromisión indebida en el ámbito personal o familiar del sujeto que conlleva la revelación de asuntos privados, el empleo de su imagen o de su nombre, o la perturbación de sus afectos o asuntos más particulares e íntimos relativos a su sexualidad o salud, con o sin divulgación en los medios de comunicación. Se ha considerado doctrinariamente, que constituyen aspectos del ámbito privado, los asuntos circunscritos a las relaciones familiares de la persona, sus costumbres y prácticas sexuales, su salud, su domicilio, *sus comunicaciones personales*, los espacios limitados y legales para la utilización de datos a nivel informático, las creencias religiosas, los secretos profesionales y en general todo "comportamiento del sujeto que no es conocido por los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación" que éstos tienen de aquel.

El derecho a la intimidad proveniente de la noción de intimidad, *privacy*, *riservatezza* o *vie privé*, tiene por objeto dotar a las personas cobertura jurídica frente al peligro que supone la informatización de

sus datos personales, sin el afán de vedar toda intromisión en las esferas de la vida que la persona se reserva para sí; sino facultándolo para permitir o no y el de controlar el uso que de su información. En relación a este aspecto del derecho inviolable e inalienable de intimidad, el Tribunal Constitucional Federal Alemán sentenció el 15 de diciembre de 1983 lo que configuró el llamado “*derecho a la autodeterminación informativa*”, mencionado anteriormente, y que faculta al individuo a decidir básicamente por sí mismo y dentro de qué límites procede revelar situaciones referentes a la propia vida. Siendo este derecho extensivo a la protección de los datos frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos por medios informáticos, lo que se conoce como libertad informática.

Una de las causas que provocó esta sentencia, relacionada en el párrafo anterior, fue debido a que en países como Francia, Suecia, Alemania, Noruega, Austria y Dinamarca elaboraron desde la década de los años 1970, instrumentos legislativos que protegieron al individuo del mal uso de su información con apoyos informáticos.; aunque de forma primitiva, pero que han ido evolucionando conforme los mismos avances tecnológicos. Así mismo, las Constituciones españolas, portuguesa, colombiana y peruana, entre otras determinan en términos generales que: la correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas mediante orden judicial, en los casos y formalidades que establezca la ley.

En el albor del siglo XXI existe una sociedad multinacional, que desconoce (debido a su estructura física), las fronteras impuestas por los políticos; quienes al verse rebasados por una sociedad intangible (que fluyen y se desenvuelven a través de líneas telefónicas, satélites, fibra óptica, etc.), han determinado que la interacción entre sus miembros debe ser regulada de forma que garantice en buena manera las nuevas relaciones de la sociedad en la era de la informatización, sin olvidar que dentro de estas nuevas legislaciones debe prevalecer las garantías de libertad, contenidas en el derecho a la intimidad; ya que como usuarios de internet tenemos derecho a que se nos compruebe con fundamentos legales, que las nuevas normas jurídicas armonizan con las relaciones propias que son derivadas del uso de la Red internet.



2.2. Generalidades del derecho a la privacidad

Actualmente, todos los individuos de manera voluntaria proporcionan sus datos personales a distintas instituciones de carácter público o privado, por diversos motivos. Si se utiliza apropiadamente dichos datos, esto permite que se convierta en información útil para la consecución de determinados objetivos. Por el contrario si estos datos se utilizan de manera errónea, pueden convertirse en una amenaza contra la dignidad de los hombres, debido al uso arbitrario y malicioso de la misma.

Por lo vulnerable de señalar en la red nuestros datos, estos deben ser protegidos legalmente contra el acceso de quienes no estén autorizados. Esta necesaria protección es un límite al manejo de la informática ante el temor de que pueda atentar contra la privacidad de los ciudadanos y que pueda restringir el ejercicio de sus derechos.

Como se sabe, una base de datos, esta compuesta por todo tipo de información aportados por las personas para determinados fines. Pero también existe una gran variedad de medios a través de los cuales se puede acceder y recopilar la información de las personas sin su consentimiento expreso, tal como sucede en algunos sitios de internet que cruzan datos de las personas que las visitan y conforman un perfil del interesado. La existencia de enormes bases de datos que contienen mucha cantidad de información referida a las personas, es una consecuencia de la informática y sin la cual sería imposible su existencia.

Lo importante es la finalidad para el cual se usara la información allí almacenada para evitar que seamos vulnerados en nuestros derechos elementales, como lo es el de la privacidad.

La cuestión es aun mas grave si especulamos que esas bases de datos pueden ser atacadas por *crackers*, quienes son aquellos aficionados a la computación que obtienen



accesos no autorizados (ilegalmente) a los sistemas de computación, robando o destruyendo datos, y que buscan información para si o para terceros, para su venta.

La doctrina especialista en el tema, esta basada en la protección hacia las personas, contra la posible utilización por terceros de sus datos personales susceptibles de tratamiento automatizado para confeccionar una información que afecte a su entorno personal, social o profesional en los límites de su privacidad e intimidad.

Actualmente la protección de datos esta prevista por las innovadoras legislaciones mediante el derecho a la intimidad y la privacidad por ende, y su transmisión telemática cuando aparece una nueva relación entre datos y personas que necesitan ser protegidos mas allá de las normas básicas a la privacidad.

Se esta regulando en base a que esa invasión a la privacidad no genere situaciones de discriminación por razones de salud, raza, ideas, costumbres y datos que pudieran llegar a limitar nuestros derechos básicos.

Por bases de datos privadas, entendemos aquellas que contienen los datos que tienen regulados situaciones o circunstancias en que la persona se ve obligada a darlos o ponerlos en conocimiento de un tercero, debiendo impedir su difusión y respetar la voluntad de secreto sobre ellos. Agregados también los datos personales de carácter íntimo, relacionados a los datos en que la persona puede proteger su difusión frente a cualquiera, para evitar así la invasión a su privacidad; ya estos datos son considerados y llamados sensibles en la Constitución Nacional de Colombia, la cual regula que: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer a actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"

Estos derechos de privacidad e intimidad, son protegidos esencialmente por el Habeas Data, considerado hoy como uno de los más importantes derechos fundamentales,

especialmente por el desarrollo de la informática y las demás tecnologías modernas, tiende a la protección de la información y las comunicaciones, específicamente a la protección de los datos personales, en especial a las ideas políticas, creencias religiosas, salud física o mental, comportamiento sexual de los individuos y *la autodeterminación informática*.

Con el avance que ha alcanzado nuestra sociedad, podríamos decir que una de las mas frecuentes violaciones de los derechos humanos la constituyen las actuaciones de entidades particulares o públicas que tienen por objeto recopilar información confidencial o personal de los individuos, sin que el dato sea verificado, ni conocido por la persona afectada por el mismo o ilegalmente manipulado. Igualmente este manejo informático del dato impide la actualización y el olvido con que la persona está sujeta irredimiblemente a soportar la carga de su pasado o de un uso impropio de la información confidencial o de sus registros informáticos, para ser utilizada como medio de presión para alcanzar fines desleales o propósitos ilícitos.

2.3. Análisis del fundamento legal guatemalteco de los derechos a la intimidad y a la privacidad

El derecho a la intimidad dentro de los medios electrónicos, debe de radicar en el poder decidir accionar contra quienes han llevado a cabo hechos ilegítimos que afecten directamente la vida privada y familiar o que den como consecuencias accesos indebidos por medio de investigaciones ilícitas a nuestros datos privados y reservados. Es decir, debe existir mecanismos que provean a las personas la seguridad de sentir que su espacio íntimo se encuentra resguardado y protegido frente a lo que pueda accionarse en el mundo informático, específicamente en la red de internet, aunque algo difícil de lograr pues cada día se conocen de nuevos medios tecnológicos que permiten la clara intromisión a la vida privada de los ciudadanos. Siendo claros y consientes, esta penetración a nuestra vida privada puede provenir tanto del sector público como del privado, ya que en ambos existe un el empleo abusivo de la tecnología, olvidándose que la misma esta al servicio de las personas y no contra de ellas.



En un plano nacional, en nuestro país la Constitución de la República de Guatemala, en el Artículo 23 referente a la inviolabilidad de la vivienda al garantizar que nadie puede penetrar en morada ajena sin permiso de quien la habita, salvo por orden escrita de juez competente y en la que se indique el motivo de la diligencia y nunca antes de las seis de la mañana y después de las dieciocho horas, y tal diligencia siempre se llevara a cabo en presencia del interesado o de su mandatario. Se menciona este artículo pues en él esta inmersa la protección al derecho de intimidad de las personas, que incluye la dignidad de las personas y guarda estrecha relación con el derecho a la seguridad, se destaca que para accesar a ese espacio privado como el la vivienda, debe existir el permiso de quien la habita o en su defecto una orden judicial. Este derecho a la intimidad de los guatemaltecos, quedo claramente establecido cuando la Corte de Constitucionalidad estima que la vivienda se va a referir directamente a la esfera privada de acción de las personas, que incluyen sus actividades profesionales, negocios o empresas, entendiendose entonces que para ingresar al espacio privado de las personas será siempre necesaria la autorización del morador.¹

Lo anterior en materia de derecho de intimidad a nivel general. Ahora, si se enfoca a nivel particular, encontramos que en el Artículo 24 de la Constitución de la República de Guatemala, los guatemaltecos gozamos del derecho a la inviolabilidad de correspondencia, documentos y libros. Dicho artículo, señala literalmente que: **“La correspondencia de toda persona, sus documentos y libros son inviolables.** Sólo podrán revisarse o incautarse, en virtud de resolución firme dictada por juez competente y con las formalidades legales. **Se garantiza el secreto de la correspondencia y a las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna.**

Cierto es, entonces que en Guatemala, el fundamento legal de carácter constitucional existe en cuanto al poder incluir en la legislación ordinaria, normas que tiendan a garantizar la privacidad e intimidad de los ciudadanos, al utilizar estos, las últimas tecnologías a su alcance. Específicamente se podría proponer un proyecto de ley

¹ Constitución Política de la República de Guatemala, y su interpretación por la Corte de Constitucionalidad.



vanguardista que luche contra la practica del envío masivo de correos electrónicos no solicitados o no deseados, recordando que para que esto se lleve a cabo, los spammers utilizan ilegalmente bases de datos de las personas y luego con ella en mano invaden nuestra correspondencia con mensajes basura e incluso enviando archivos que dañan nuestro equipo físico y que pueden atentar contra nuestra seguridad al perjudicar información que solo nos compete a nosotros o a nuestras empresas.

En el Congreso de la República de Guatemala existe ya al menos un Proyecto Ley de Habeas Data, el cual tristemente ha quedado en eso un proyecto. Por lo que creo conveniente volver a retomar el tema de la protección de datos personales de los guatemaltecos y proponer a la vez una norma que tienda a combatir al spam. Recordemos que nuestro país ha tenido un avance en los aspectos culturales, educacionales y sobre todo económicos y que lucha a diario por ingresar en los estándares de la economía global, misma en donde se demanda apertura en aplicación de legislaciones modernas que incluyan los hechos ilícitos que han surgido en los últimos tiempos generados por las nuevas tecnologías. Estas normas jurídicas que se proponen ya no son un capricho de estudiante, sino más bien se presenta como una propuesta para darle salidas concretas a casos ya reales a nivel mundial que no se pueden dejar a un lado en nuestro país; para el desarrollo económico y social en el que se quiere situar, es por ende, necesario abrir la mente a nuevos cambios nos solo sociales, sino lo más importantes percibirlos en el Derecho.

2.4. Relación actual de los derechos a la intimidad y privacidad en contra posición al correo electrónico no deseado o no solicitado

Con lo ya anotado, podemos ver que en la actualidad existe una nueva modalidad de invadir la intimidad y privacidad de las personas, en otro ámbito de esa esfera, a través de la utilización de los datos personales para distintos fines muy ajenos para los cuales se ha prestado los mismos. Esto debido a la facilidad que hoy por hoy existe por la informatización de los datos, a ese tratamiento de rapidez con los que se manejan y la poca o casi nula legislación efectiva al respecto.

Resulta evidente que el envío de publicidad no deseada como mecanismo de marketing directo es un fenómeno que antecede con creces a internet y el spam. Diariamente las casas y departamentos son bombardeadas con cartas, que ofrecen servicios no solicitados. Asimismo, aunque quizás con menor frecuencia, no es extraño recibir o recuperar de la contestadora telefónica llamadas a través de las cuales, una vez más, se ofrecen servicios no solicitados. Con estos argumentos muchos especialistas podrían preguntarse por qué entonces no tratar al spam como una más de estas prácticas; la respuesta son distintas, pero una en general podría ser básicamente que mientras las solicitudes comerciales no deseadas han sido un hecho de la vida por un largo tiempo, nunca antes ellas habían amenazado la viabilidad de todo un modo de comunicación; ya que ahora se utiliza el spam, como una especie de “ECO”, esto en relación a la imagen proyectada como eco que se encuentra en el Libro *Serendipities, Language and lunacy*²; allí “ECO” se relata como toda la tradición medieval convenció a Europa de la existencia del unicornio, un animal que asemejaba un delicado y gentil caballo blanco con un cuerno sobre su hocico. Como encontrar unicornios en Europa no resultaba sencillo, la tradición decidió que estos animales debían habitar en países exóticos. Marco Polo, como habitante de la Europa medieval también se empapó de esta tradición, así cuando viajó a China estaba preparado para encontrar unicornios y, de hecho, durante su viaje los buscó afanosamente. Nos cuenta Eco que el encuentro se produjo mientras el viajero volvía a casa, en la isla de Java. Siendo Marco Polo un cronista honesto no pudo dejar de advertir que estos unicornios presentaban algunas diferencias con aquellos que anunciaba la tradición europea. De acuerdo a la relación de ECO: ellos no eran blancos sino negros. Su piel asemejaba a la de los búfalos y sus abdómenes eran tan abultados como los de los elefantes. Sus cuernos no eran blancos sino negros, sus lenguas eran erizadas y sus cabezas asemejaban a las de los jabalíes salvajes. Con esta anécdota, visualizamos claramente que si tratamos al spam simplemente como otra forma de comunicación directa equivaldría a tratar a un rinoceronte como si fuera un unicornio.

² Orion Books. Londres. Edición 1998, pág. 79



El spam, presenta una ventaja de carácter económico, ya que los los mecanismos de marketing directo permiten llegar a los consumidores en términos que, al menos estadísticamente, llamarán su atención con mayor intensidad que mecanismos alternativos como publicidad en las calles o avisos en televisión. Lo cual conlleva un costo financiero, ya que en el caso del envío de publicidad por correo regular, por ejemplo, es el avisador quien soporta la gran mayoría –sino todos- los costos del envío de la publicidad. De esta manera se invertirá en marketing directo en la medida que la ganancia proveniente de la respuesta de los consumidores supere a los costos de alcanzar a los consumidores. En el envío de publicidad masiva por correo electrónico, sin embargo, la ecuación entre costos y beneficios es diferente, pues es el usuario del servicio de la red, quien ha pagado por dicho servicio para su uso personal, y el cual termina pagando monetariamente hablando, los costos de la publicidad enviada a través de los correos electrónicos no deseados o no solicitados, llamados spam.

Con lo manifestado, se ve que ahora se utiliza el avance tecnológico no solo para agilizar y facilitar la vida en sociedad, sino se esta aprovechando además, para otros fines, contrarios a los que nosotros hemos autorizado específicamente nuestra información. Con estas practicas, se adentran en nuestros datos personales en general, y en particular a la dirección personal de nuestro correo electrónico, la cual utilizan con fines ya sean publicitarios, políticos, religiosos, etc., correos que incluyen al final de cuentas información que no hemos solicitado, y que lejos de contribuir en algo, no solo ocasionan perdida de tiempo, y dinero, sino además, se corre el riesgo de que al ingresar a nuestro correo, nos dañen el sistema y con ello perdamos información valiosa.

Actualmente en lo que se refiere al spam o correos electrónicos no deseados o no solicitados, los legisladores modernos contemplando la nueva forma en que se violan los derechos de privacidad e intimidad de las personas, se han reunido con esta preocupación y ya por ejemplo en la norma colombiana, señalaron que queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido



solicitadas o expresamente autorizadas por los destinatarios de las mismas; y además se ha establecido que cuando por el mal uso del internet o fax se atente contra el patrimonio moral de las personas, se ponga en riesgo su vida o atente contra la seguridad y la estabilidad económica de las empresas, cualquiera que fuese su actividad, las autoridades competentes pueden, con fundamento en los libros de registro, aplicar a los responsables el rigor de las leyes preexistentes en materia civil, comercial o penal para castigar a dichas personas.

España es uno de los pocos estados vanguardistas en relación al tema del spam, pues prohíbe absolutamente esta mala técnica de enviar correos electrónicos (gracias a dos leyes claras que regulan la utilización del spam y la el origen de los datos ilícitos sin autorización del propietario), que imponen en ambos casos severas sanciones a los responsables.

Estos casos, por mencionar algunos países vanguardistas en la protección de los derechos de intimidad y privacidad en la nueva era de la sociedad de la información.

Se puede concluir, que si bien es cierto que los ciudadanos de cualquier Estado, tienen el derecho a ser informados y de utilizar los medios de la tecnología informatizada, estas relaciones conjugadas por todos, deben mediar en armonía y legalidad, es decir, no se puede vulnerar los derechos de intimidad y privacidad de las personas sin que exista una autorización previa y expresa para utilizar en determinado fin, nuestros datos personales, en el caso del presente estudio, nuestro dato personal de la dirección de correo electrónico.

2.5. Lineamientos para prevenir el correo electrónico no deseado o no solicitado

Como hemos visto la dirección de correo electrónico es el medio más utilizado para registrar la identidad de una persona en internet y generalmente sirve de base para la acumulación de información en torno a la misma. En muchas ocasiones contiene información acerca de la persona como el apellido, la empresa donde trabaja o el país

de residencia. Esta dirección puede utilizarse en múltiples lugares de la red y puede ser conseguida fácilmente sin nuestro conocimiento, por lo que es necesario seguir una serie de normas para salvaguardar nuestra privacidad e intimidad.

A continuación se presentan algunos consejos para prevenir los correos electrónicos no deseados no solicitados:

- **Ser cuidadoso al facilitar la dirección de correo:** proporcionar únicamente la dirección de correo a aquellas personas y organizaciones en las que confía y aquellas con las que quiera comunicar.

- **Utilizar dos o más direcciones de correo electrónico:** es aconsejable crear una dirección de correo electrónica, que será la que se debe proporcionar en aquellos casos en los que no se confíe o conozca lo suficiente al destinatario. De este modo, su dirección personal será conocida únicamente por sus amigos o por sus contactos profesionales, con el ahorro de tiempo que implica no tener que separar correos importantes de aquellos no deseados. Lo mismo se recomienda a la hora de utilizar servicios de mensajería instantánea.

- **Elegir una dirección de correo poco identificable:** los *spammers* obtienen las direcciones de correo electrónico de formas muy diferentes. Así navegando por la red, en salas de Chat (salas de conversación por internet), o incluso en directorios de contactos o usando la ingeniería social. A veces compran incluso listas de correo electrónico en sitios web que venden los datos de sus clientes. Y, cuando todo esto falla, simplemente conjeturan. Las direcciones de correo electrónico que se refieren a una persona como tal, suelen contener algún elemento que les identifique y son fáciles de recordar. Esta forma de crear el correo permite a los *spammers* intuir las direcciones de correo electrónico. Por ejemplo, si el nombre del usuario es Juan Pérez, el spammer probará con las siguientes opciones: juanperez@..., j.perez@..., jprz@..., juan.prz@..., etc. Los *spammers* incluso cuentan con programas que generan automáticamente posibles direcciones de correo. Pueden crear cientos de

direcciones en un minuto, ya que trabajan utilizando diccionarios, es decir, una lista de palabras que se suelen usar en las direcciones de correo. Estos diccionarios suelen contener campos como los siguientes:

- Alias
- Apellidos
- Iniciales
- Apodos
- Nombres de mascotas
- Marcas
- Signos del zodiaco
- Meses del año
- Días de la semana
- Nombres de lugares
- Modelos de coches
- Términos deportivos

Estos programas simplemente introducen datos en cada uno de estos campos e intentan varias combinaciones con todos ellos. Además añaden letras y números en las combinaciones, ya que se suelen introducir fechas de cumpleaños, edades, etc. Para crear una dirección de correo electrónico y reducir el envío de spam, sería conveniente no introducir campos que sean potencialmente útiles por el *spammer*.

- **No publicar la dirección de correo:** no se debería anunciar la dirección de correo en buscadores, directorios de contactos, foros o páginas web. En el caso de los chat, no se debe mostrar la dirección de correo electrónico en las listas de usuarios y no se debe comunicar a desconocidos. Cuando envíe correos en los que aparezcan muchas direcciones, envíelas usando BCC o CCO (con copia oculta) para no hacer visibles

todas las direcciones. Si es necesario facilitar la dirección de correo electrónico en alguna web, envíela en formato imagen o escriba 'at' o 'arroba' en lugar de @. De este modo se puede evitar que lo capturen los programas creadores de spam. Asimismo, si reenvía un correo, elimine las direcciones de los anteriores destinatarios: son datos de fácil obtención por los *spammers*.

- **Leer detenidamente las políticas de privacidad y las condiciones de cancelación:** si se va a suscribir a un servicio *on line*, o a contratar un producto, revise la política de privacidad antes de dar su dirección de correo electrónico u otra información de carácter personal. Puede que esta compañía vaya a ceder los datos a otras o a sus filiales y observe que no le suscriben a boletines comerciales, por lo que es conveniente saber la política de alquiler, venta o intercambio de datos que han adoptado tanto su proveedor de acceso a internet como los administradores de los directorios y listas de distribución donde esté incluido. Capture la pantalla y páginas en las que compra y conserve los datos identificadores. Además, lea los mensajes sospechosos como texto y no como html y desactive la previsualización de los correos. No se debe en dudar en ejercer los derechos de acceso y cancelación sobre sus datos ante estas empresas.

- **Sensibilizar a los niños sobre la utilización del correo y la mensajería instantánea:** los niños son objetivos ideales para promocionar información sobre la composición y las prácticas de consumo del hogar. Por eso es importante recordarles algunos consejos prácticos que ayudarán a evitar que el niño aporte datos personales. Además, mediante la dirección de correo electrónico no se puede saber quien es el destinatario de correos que pueden tener contenidos no aptos para los niños.

2.6. Lineamientos para reducir el correo electrónico no deseado no solicitado

Cuando nos encontramos con la situación de que ya estamos recibiendo estos correos electrónicos que no hemos solicitado o no deseamos, es casi imposible detenerlo completamente sin recurrir a un cambio de dirección de correo electrónico.

De todas formas, la Agencia Española de Protección de Datos, presenta las siguientes consejos para reducir la recepción de correos electrónicos no solicitados o no deseados, a manera de recomendaciones para que puedan ser aplicados y con ello contribuir a la reducción de la proliferación del “correo basura”.

- **No es conveniente contestar al spam:** responder a dichos correos informa al remitente de que la dirección está activa, lo que puede animar tanto a éste como a otros *spammers* a enviar todavía más mensajes. Es conveniente desactivar la opción que envía un acuse de recibo al remitente de los mensajes leídos del sistema de correo electrónico. Si un *spammer* recibe dicho acuse sabrá que la dirección está activa, y lo más probable es que le envíe más spam.
- **No presione o accese sobre los anuncios de los correos basura:** entrando en las páginas web de los *spammers* podemos demostrar que nuestra cuenta de correo está activa, con lo que puede convertirse en un objetivo para nuevos envíos. Por otra parte, los gráficos e imágenes (también llamados *web bugs* –incluidos en los correos basura pueden proporcionar al *spammer* no sólo la información de que el mensaje ha sido recibido, sino también datos de carácter personal como la dirección IP.
- **Utilice filtros de correo, es decir, programas de filtrado de correo electrónico:** los programas de gestión de correo electrónico, así como muchas páginas web de correo, ofrecen la posibilidad de activar filtros que separan el correo deseado del spam. Las principales desventajas son que puede confundir correos legítimos con mensajes basura. Cada vez se fabrican programas más avanzados en este campo, que en muchos casos pueden ser descargados libremente de internet. Estos filtros reciben instrucciones para definir que tipo de correos se quiere recibir y cuales son considerados como spam.
- **Filtros basados en listas negras:** muchos proveedores de internet ofrecen soluciones que pueden llegar a ser muy efectivas a la hora de bloquear el spam.

Utilizan combinaciones de listas negras y escaneado de contenidos para limitar la cantidad de spam que llega a las direcciones. El principal inconveniente es que, en ocasiones, bloquean correos legítimos, y además suelen ser servicios de pago. Para más información, consulte con su proveedor.

- **Mantenga al día su sistema:** los ordenadores personales requieren de un mantenimiento. La mayoría de las compañías de software distribuyen actualizaciones y parches de sus productos que corrigen los problemas detectados en sus programas. Estas actualizaciones suelen estar disponibles en las páginas web de los fabricantes, y generalmente su descarga e instalación es gratuita. Por otra parte, los usuarios deberían utilizar programas **antivirus** para protegerse contra estos perniciosos programas, capaces de destruir todos los archivos de un ordenador, y que cada vez son más utilizados por los *spammers*. Asimismo, es muy recomendable la instalación de un **cortafuegos** para monitorizar lo que ocurre en el ordenador.

Todas las recomendaciones tanto para prevenir el spam, como para reducirlo, se describen en los principales servicios de internet, así como la identificación de los posibles riesgos para la privacidad y lo que puede ocasionar y los consejos que se proponen a los usuarios, por lo que siempre es recomendable verificar dicha información.

CAPÍTULO III

3. Se debe legislar a favor de garantizar los derechos a la intimidad y privacidad en el contexto legal guatemalteco, con relación al spam o correo electrónico no deseado

3.1 Análisis jurídico económico del abuso de direcciones de correo electrónico con fines publicitarios

El problema de los mensajes no deseados que circulan en internet, los cuales son mejor conocidos como spam o correos electrónicos no deseados, no salen gratis, y son los proveedores de acceso a internet los primeros en pagar por el uso abusivo de sus redes. El spam produce unas pérdidas anuales a nivel mundial que algunas estimaciones sitúan entre 3, 000 y 4,000 millones de dólares, según los datos manejados en la Conferencia Anti-Abuso de Correo celebrada en Londres, en el año 2007.

Servicios como Hotmail reciben unos 2,000 millones de correos basura diarios, y a nivel mundial son unos 8,000 millones los mensajes de publicidad no deseada que se envían a millones de buzones del mundo.

La cantidad de mensajes consume el ancho de la banda de internet, espacio de almacenamiento y potencia informática que acaba costando a los proveedores entre cinco y ocho dólares anuales por cada uno de los usuarios de correo electrónico.

Las principales iniciativas para frenar el correo basura trabajan en distintas direcciones, lo que minimiza su efectividad, criticó Philippe Gerard, miembro de la dirección para la Sociedad de la Información en la Comisión Europea. Gerard ha llamado la atención de los Gobiernos sobre la necesidad de legislación para atajar el problema y favorecer el comercio electrónico.

Al respecto, los ministros de telecomunicaciones de la Unión Europea, decidieron prorrogar cuatro años el programa 'Safer Internet Plus', otorgando un reglón presupuestario de 45 millones de euros para frenar la proliferación de contenidos ilegales en internet, específicamente para combatir el spam y en especial el que contenga pornografía infantil.

Recientemente, este problema de los correos electrónicos no deseados o no solicitados, se trató en la ciudad de Ginebra, Suiza, en un encuentro promovido por la Unión Internacional de Telecomunicaciones (UIT), este organismo calificó al correo no deseado como 'una de las plagas más importantes del mundo digital, que amenaza con obstruir el correo electrónico y los servicios de mensajería instantáneos. Por este motivo ha tratado de diseñar un plan de choque, que incluye legislaciones a la vanguardia de la tecnología.

“El spam es todo un negocio”, dice Steven Linford, creador del Proyecto Spamhaus, una organización sin ánimo de lucro dedicada a detener el correo basura, en su estudio concluye que en el año 2003 se gastaron unos 11,000 millones de dólares en publicitar productos mediante el envío de correos no solicitados, según datos del Grupo Contra el Abuso del Correo. No se trata de personas que no tienen otra cosa que hacer, sino de bandas criminales organizadas para las que el spam es un lucrativo negocio,' explica Linford., Estados Unidos y China son actualmente dos de los principales países de los que sale el correo basura que inunda internet, pero Rusia comienza a asomar como potencia exportadora de correos no deseados. Las bandas criminales de este país están comenzando a entrar en el negocio del correo basura, explica Linford, ya que ven el crecimiento económico y la generación de ganancias que producen.

Es tan peculiar y rentable este negocio, que los teléfonos celulares, pueden ser el próximo lugar al que se traslade la plaga de los mensajes no deseados, al menos eso es lo que muchos operadores comienzan a temer. Los mensajes de texto y los nuevos mensajes multimedia podrían ser las próximas víctimas. La diferencia con el correo electrónico es notable, ya que el canal móvil tiene un ancho de banda más limitado



(sólo 160 caracteres de texto o videos y fotos pequeñas) y hay que pagar por cada mensaje, pero esto no quita para que ya hayan surgido algunos servicios abusivos, incluso en España. Entre ellos se encuentran las llamadas perdidas de un solo timbre que incitan a devolver una llamada a un número de tarifa especial, mensajes de texto que animan a que se llame a uno de estos números prometiendo algún premio o mensajes cortos publicitarios.

La consultora estadounidense Nucleus Research ha publicado un alarmante estudio sobre los efectos del spam. La firma ha sondeado la experiencia de 82 grandes compañías y concluye que el tiempo que gastan sus empleados en eliminar correo basura de sus buzones les cuesta una media de 1,934 dólares anuales por persona.

El tráfico de spam está doblando en 2004 las cifras del año anterior y las inversiones privadas para frenarlo han topado con el citado incremento, por lo que el problema no está resuelto. El estudio de Nucleus asegura que los filtros instalados por las mayores compañías captan el 20% del spam, frente al 26% del año 2003. Por su parte, se prevé que en 2006 circularán cada día por la red unos 22,000 millones de estos correos electrónicos, frente a los 16.700 millones de hoy.

La ventaja de los mecanismos de marketing directo es que permiten llegar a los consumidores en términos que, al menos estadísticamente, llamarán su atención con mayor intensidad que mecanismos alternativos como publicidad en las calles o avisos en televisión. Lo anterior, sin embargo, posee costos. En el caso del envío de publicidad por correo regular, por ejemplo, es el avisador quien soporta la gran mayoría –sino todos- los costos del envío de la publicidad. De esta manera se invertirá en marketing directo en la medida que la ganancia proveniente de la respuesta de los consumidores supere a los costos de alcanzar a los consumidores. En el envío de publicidad masiva por correo electrónico, sin embargo, la ecuación entre costos y beneficios es diferente, pues es quien envía las comunicaciones. En general los costos que asume quien envía el spam son el de encontrar un proveedor de servicios de internet suficientemente inocente, la composición del mensaje y el establecimiento de un sistema de



procesamiento de pago por los bienes o servicios, en el caso que los provea el mismo o bien la contratación de este servicio en caso contrario. El costo marginal de enviar un correo electrónico más es prácticamente inexistente, por lo tanto, los incentivos del emisor son enviar tantos mensajes como sea posible.

Junto a los costos marginales prácticamente nulos, el envío masivo se justifica porque la tasa de retorno obtenida por el emisor dependerá del número de correos que envíe. Si se suman ambas cosas el resultado es que aún resulta económicamente razonable enviar diez millones de correos electrónicos aún si las respuestas son pocas. Actualmente en promedio un spammer puede enviar mensajes a través del correo electrónico a un millón de personas por la suma de cien dólares. A este precio, aún si un solo receptor entre diez mil responde, el spammer puede obtener beneficios y olvidar a los restantes nueve mil novecientos noventa y nueve enojados receptores de mensajes no deseados. Esto es ya que el correo electrónico no deseado o no solicitado es barato y produce resultados; y en ese sentido, constituye una práctica absolutamente inédita, ya que en la actualidad no existe otra forma de publicidad que se le pueda comparar.

Para visualizar en porcentajes, los perjuicios económicos del spam, tenemos que según informes recientes de Nectom, empresa de seguridad en internet, 14% de los correos electrónicos corresponden a spam. Netcom, un proveedor de servicios de internet (ISP), y reporta que el spam incrementa los costos de soporte entre un 15% y un 20%, los de administración alrededor de un 20%, los de descarga de correos entrantes en un e10%, reduce el espacio en el disco alrededor de un 15% y aumenta los costos totales por equipos entre un 10 y un 15%. Incluyen en su informe que según las cifras entregadas por la Federal Trade Commision, en 1998, se recibía 1, 500 reclamos diarios por spam. En el caso America Online, Inc., empresa proveedora de internet, “alegó que dicha práctica de enviar correos electrónicos no deseados había producido, entre otras consecuencias, 50, 000 quejas de sus afiliados”.³

³ Ambos datos citados en FASANO, Christopher: Getting Rid of Spam.

Una práctica común de los spammers consiste en utilizar direcciones de correo falsas, pertenecientes a proveedores de servicios que no poseen relación con el spammer. Para quien recibe el correo electrónico, sin embargo, el proveedor de servicios que aparece en la dirección del correo es quien permite el uso de sus instalaciones para el envío de correos no solicitados. Junto a la pérdida de reputación y prestigio de los proveedores del servicio de internet, dichos proveedores pueden verse expuestos a ataques de algunos de los receptores de la publicidad no deseada.

Junto a los proveedores de servicios, los segundos afectados son los usuarios de internet, ya que quienes reciben correos no deseados en su casilla electrónica utilizan su tiempo y dinero para procesarlos. Como se viene advirtiendo, si una persona no dispone de filtro, o quien envía los correos electrónicos ha encontrado una forma de eludir el filtro, el receptor de los correos electrónicos debe ocuparse de ellos. Ocuparse de ellos toma tiempo por el cual el usuario debe pagar y el espacio físico que utiliza el mensaje puede disminuir la capacidad de un sistema o consumir espacio que, de otra manera, sería necesario para el procesamiento de tareas más importantes. En este sentido, el receptor de correos no solicitados esta pagando parte del costo por algo que ella o él no desea, ya sea que este costo sea monetario o en otros recursos.⁴

Además de los proveedores de servicios y a los usuarios, el spam puede producir un daño más global a la Red. La proliferación incontrolada del spam podría tener un cierto efecto paralizante sobre internet, ya sea porque el contenido de los mensajes de publicidad buena parte de ellos sobre sitios pornográficos con lenguaje extraordinariamente explícito o imágenes suficientemente elocuentes⁵ disuade a los usuarios de interactuar en la Red por temor a que sus datos sean recogidos por spammers o por que el número de correos electrónicos no solicitados simplemente sature la Red. En este sentido GAUTHRONET Y DROUARD reportan que: Existen actualmente 234 millones de usuarios de internet y es posible que alcancen los 300

⁴ MIKA, Karin: Information v. Commercialization: The Internet and Unsolicited Electronic Mail,

⁵ Según información proporcionada por CISCO Systems Chile durante 1999, el 30,2% de los email no solicitados poseían contenido pornográfico, 29,6% consistía en ofertas para "hacerse rico", 23,5% buscaba vender otros productos o servicios, 9,9% ofrecía productos relacionados a la salud y 3,3% ofrecía entrada a sorteos o a juegos de azar.



millones a fines del 2000. Si se asume que tarde o temprano cada empresa de "marketing e-mail" adquirirá la capacidad técnica de transmitir 100 millones de correos electrónicos al día, los usuarios de internet podrían quedar potencialmente sobrepasados por la inundación de mensajes –200 emisores que posean esa es posible que alcancen los 300 millones a fines del 2000. Si se asume que tarde o temprano cada empresa de "marketing e-mail" adquirirá la capacidad técnica de transmitir 100 millones de correos electrónicos al día, los usuarios de internet podrían quedar potencialmente sobrepasados por la inundación de mensajes –200 emisores que posean esa el envío de correos electrónicos masivos es atractivo como mecanismo de avisaje por dos razones. La primera de ellas tiene que ver con su efectividad, la segunda con sus costos. El spam entonces es un modo eficiente y barato de publicitar bienes y servicios.

El ya famoso cartero tradicional comercial que se filtraba en los portales físicos para llenar los buzones con publicidad, esta perdiendo actualidad, frente al cartero electrónico. Ya que además de costar dinero, su radio de acción es muy limitado; por lo que las empresas se dieron cuenta que a través del correo electrónico se pueden enviar más mensajes, a mucha más gente y mucho más lejos y por muy poco dinero.

Basta con tener un listado de direcciones, escribir un mensaje genérico y disponer de un módem a básico para la computadora para mandar cientos de miles de mensajes por hora. Pero lo que realmente sucede, es que con el envío masivo de estos correos electrónicos se ocasiona que se convierte al sistema en una verdadera plaga de la red, que inunda servidores, congestiona la red y termina desesperando a los usuarios.

Actualmente, las formas o métodos para acceder a bases de datos con direcciones de correo son variadas, lo más sencillo es a través de los grupos o foros de discusión conocidos como USENET de donde se recopilan la mayoría de direcciones electrónicas. Existen personas exclusivas que se dedican a la recopilación de direcciones electrónicas de forma ilegal, pues no cuentan con la autorización de los titulares de dichas direcciones, con el único fin de venderlas a terceras personas dedicadas a la publicidad o a diversos negocios para sus promociones.



El spam o correos electrónicos no deseados utiliza recursos ajenos y de forma ilegal para sus intereses personales, que otras personas acaban asumiendo el costo financiero. Por ejemplo American On Line (servidor de internet) recibía 1,8 millones de mensajes al día de Cyber-promociones (empresa dedicada al envío masivo de correos electrónicos no deseados con fines lucrativos) hasta que consiguió una orden judicial para prohibirlos, ya que a un usuario le lleva unos 10 segundos identificar el correo basura y tirarlo, sólo en AOL se gastaban más de 5.000 horas de conexión al día por culpa del spam, lo cual perjudicaba además su banda de transmisión.

La forma más sutil de tratar de confundir a los usuarios de la red, es hacer parecer al correo basura como correo de cualquier otro tema importante, para que los filtros no lo detecten, por los que se dedican a este envío de correos electrónicos utilizan trucos para disfrazar el origen del mensaje. Una estrategia habitual consiste enviar los correos electrónicos a través del servidor de un tercero que, para colmo, es el que sufrirá las iras del los usuarios-víctimas. Estos correos electrónicos no deseados o no solicitados, llamados spam, contienen en su gran mayoría, información de:

Cadenas de cartas. Esas de 'reenvíelo a 10 personas y sobrevivirá'.

- Negocios piramidales, incluido el multinivel Marketing
- Otros mensajes tipo 'Hágase rico rápidamente'.
- Anuncios de webs pornográficos o líneas eróticas.
- Programas para acumular direcciones y hacer spamming.
- Oferta de acciones de empresas desconocidas.
- Remedios milagrosos.
- Niños/Ancianos muy enfermos. Penurias y tragedias varias.
- Falsas amenazas de virus.
- Programas piratas (warez).

Toda esta información con el fin de generar ingresos lucrativos a terceros, que se dedican a la captura de direcciones electrónicas para su venta a empresas de mercado



y publicidad, o ingresos a las mismas empresas de negocios diversos.

En Mayo del año 2005. las empresas, ChooseYourMail junto con CAUCE (Committee Against Unsolicited Commercial Email), FREE (Forum for Responsible and Ethical Email) y SAFEeps crearon el spam Recycling Center (SRC) para que los usuarios reenvíen su correo basura, con el objeto de detectar los servidores de donde provenían dichos correos, así como para verificar su contenido, teniendo como respuesta que recibieron del 11 de mayo y el 1 de julio 2005 se repartía como sigue:

Los mensajes relacionados con la pornografía se colocan en cabeza con un 30,2%, seguidos muy de cerca por los que ofrecen ganar dinero rápido y fácil (29,6%), de los cuales el 12,5% ofrecen técnicas de spam, desde listados de direcciones de correo hasta programas de spamming. El tercer grupo engloba todos los mensajes que venden productos o servicios (decodificadores, equipos y programas, acciones, seguros, etc.) con un 23,5%. Un 9,9% vendía medicamentos (un 21,4% de Viagra o similares) y un 3,3% estaban dedicados a diversos juegos de lotería y apuestas.

Con estos datos se concluye que el spam es un negocio rentable, ya que por ejemplo en España el 84% del correo que llega a los correos electrónicos son spam, según se desprende del informe sobre amenazas de seguridad, elaborado por Symantec y referido al área de Europa, Oriente Próximo y África. Esta cifra es muy superior al porcentaje medio de la zona (66%) y de todo el mundo (59%) y coloca a España en el cuarto puesto de los países de la zona que reciben más correo no deseado, solo por detrás de Portugal, Polonia y Egipto.

Económicamente, el spam está generando costos monetarios, ya que por ejemplo en abril del dos mil siete, Nucleus Research, menciona que la epidemia del spam le está costando a la industria estadounidense 712 dólares por empleado al año. El estudio realizado por Nucleus Research, quien es un proveedor global de información tecnológica, consiste en una encuesta a 849 usuarios de correos electrónicos que fueron realizadas en el mes de marzo de dos mil siete.



Según este estudio, dos de cada tres mensajes de correos electrónicos recibidos por los empleados de las empresas son spam. Como consecuencia de esto, los empleados pierden 16 segundos identificando y eliminando el correo fraudulento. Esta pérdida de tiempo se traduce en un coste anual de 70.000 millones para la industria de Estados Unidos.

Nucleus Research estima que el tráfico total de correos electrónicos en las empresas, está saturando en un 90% por correos basura, y que sus empleados reciben una media de 21 mensajes de spam cada día.

En Guatemala, para ser específicos, existen empresas de este tipo, es decir, que se dedican al envío masivo de correos electrónicos, ya que por mil quetzales ofrecen llenar el correo electrónico de aproximadamente 300,000 guatemaltecos y que 20% de éstos responderá a la publicidad y que muchas veces hasta 60% de respuesta en tan sólo de 24 horas.

También es muy común que ahora exista otro tipo de spam muy utilizado en tiempos de elecciones, aquí por ejemplo en nuestro país, desde el año pasado se habla del papel que ha tenido la internet en las campañas de desprestigio de bancos del sistema y de candidatos. Esto es algo común, que sucede en todo el mundo. Pero a diferencia de otros países, en Guatemala estos rumores no se transmiten a través de blogs de discusión, sino a través del spam. Esto se da ya que como en Guatemala la utilización de internet ilimitado no está al alcance de la mayoría de los pobladores, los usuarios ingresan a la red lo hacen a través de cafés internet; lo que implica que la forma de comunicación más común sea el chat o el correo electrónico. Esto explica el por qué el spam se ha convertido en un método tan efectivo para difundir rumores, además de la excesiva publicidad por spam.

En Guatemala, el problema mayor se puede enfocar a que los usuarios guatemaltecos

no están informados de lo que es el spam y de sus peligros y sobre todo desconocen que el contenido de los spam no es confiable. Aparte del desprestigio que conllevan las campañas negras, el spam es peligroso porque:

1. Puede bloquear el buzón del correo, si su buzón tiene capacidad limitada
2. Puede contagiar su computadora con virus
3. Puede llevarle a páginas con cobro extra
4. Puede hacer que usted dé información personal a desconocidos

3.2. Fundamentos y puntos para legislar contra el envío de correos electrónicos no deseados no solicitados, spam

Debido a la proliferación y avance en las comunicaciones de carácter transfronterizas comerciales no solicitadas, se comienza a generar y plantear problemas de carácter jurisdiccional; llegando a que en la actualidad se reúnen países para tratar temas como la ciberseguridad; en donde se desarrollan políticas nacionales y enfoques legislativos sobre el correo basura, para lo cual se consideran las distintas políticas y legislaciones adoptadas en todo el mundo para combatir ese flagelo.

Los encargados de regular dicho problema, como lo es el envío de correos electrónicos no deseados conocidos como spam, deben decidir si incluyen el “spam” sólo en el contexto de los correos electrónicos, o si dichas leyes contemplan otras aplicaciones como, por ejemplo, el servicio de mensajes breves (SMS) de los teléfonos celulares, la mensajería instantánea (conocida como “spim”, un tipo de envíos no solicitados de mensajería instantánea), y los diarios personales por internet o bitácoras (blogs). Algunas leyes contra el correo basura, como la Directiva 2002/58/CE de la Comisión Europea, se aplican a todos los métodos de comunicaciones electrónicas, no únicamente a los enviados a través del correo electrónico. En Estados Unidos, existe una legislación que sólo se aplica al correo electrónico, mientras que las comunicaciones por SMS de los teléfonos celulares se rigen por normativas diferentes.



Uno de los principales problemas al tratar de legislar contra el spam, es que el ciberespacio no tiene fronteras basadas en el territorio ya que el costo y velocidad de envío de la transmisión de un mensaje en la internet es casi completamente independiente de la ubicación física: los mensajes pueden ser transmitidos desde cualquier ubicación a cualquier ubicación sin arruinarse, degradarse o demorarse sustancialmente más y sin que ninguna barrera física o que pueda mantener lugares y personas remotamente alejados separados unos de otros. La Red permite transacciones entre gente que no se conoce, y en muchos casos, entre gente que no puede conocer la ubicación física de la otra parte. La ubicación continua siendo importante, pero solo la ubicación dentro de un espacio virtual compuesto por las “direcciones” de las máquinas entre las cuales los mensajes y la información es seguida.

El problema del dinamismo de la tecnología y la rapidez con que se desarrolla día a día, es un desafío para cualquier normativa que intente regular la interacción social en la internet. Sabemos cómo funciona internet hoy y la forma en que se desarrollan algunas conductas que nos parecen reprobables o incluso ya tipificadas como delitos. El problema, sin embargo, es encontrar formas de fijar esas conductas en tipos que resulten suficientemente flexibles para evitar su desactualización frente a la tecnología que regulan, la cual es modificada constantemente por los avances veloces con los que cuenta.

Podemos decir, que las normas que tiendan a regular el spam o correos electrónicos no deseados o no solicitados, deberán incluir, en forma general los siguientes puntos:

- a) Definir y sancionar las actividades que constituyan spam, castigando con mayor severidad aquellas cuyo propósito o efecto sea causar daño o vulnerar la seguridad de los sistemas o equipos de informática o la información contenida en ellos;
- b) Dotar de los mecanismos necesarios de control a los usuarios del correo electrónico sobre la recepción de mensajes;

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

d) Proveer los mecanismos de control necesarios anti spam, a los proveedores de servicios de comunicaciones, así como establecer el resarcimiento legal por el eventual daño que estos puedan sufrir derivado del esta mala practica del spam.

También al momento de legislar en relación al spam, debe tenerse en cuenta qué se quiere solucionar o prevenir, si el correo basura en los buzones de los usuarios, o reducir el impacto en los servidores de correo y líneas de comunicaciones; o por el contrario se quiere combatir el spam en general por ser un problema voraz en la internet.

En función de cuales sean nuestros objetivos, debemos enfocar las posibles alternativas al problema; ya que no serán iguales las soluciones o medidas a adoptar para una empresa que para un proveedor de servicios internet que para una comunidad en general.

En función de cómo queremos reducir los efectos del spam podemos clasificar las soluciones en:

- **Precavidas:** las cuales serán normas que colaboran a evitar recibir o distribuir spam desde Empresa o Proveedores.
- **Reactivas:** en estas se hablaría de las normas que deban tomarse después que el correo (spam) haya llegado a los servidores y buzones. Como por ejemplo, las medidas actuales como las del tipo Filtros de contenidos (Content-Filter) tanto para servidores como clientes de correo; filtros que evitan el acceso a estos correos no solicitados.

- **Proactivas:** podrían ser las normas que se tomen antes que el correo (spam) llegue a los servidores.

Aunque no existe una solución ni exacta ni infalible y mucho menos global, la aplicación de todas si reducirá el impacto del spam. Claro, esto no implica que no se deban tomar medidas porque las que se tomen siempre reducirán en mayor o menor grado el impacto del spam. Y esto es debido a que las técnicas de los *spammers* cambian continuamente a medida que aparecen nuevas técnicas para evitarlo. Estas medidas son necesarias para prevenir la captura de nuestras direcciones de correo. La distribución de spam sólo es posible si se dispone de muchas de estas direcciones. La captura de direcciones escaneando páginas Web es una técnica habitual para la distribución de spam.

3.3. Legislación vigente a nivel nacional enfocada a los correos electrónicos no deseados o no solicitados spam

En el Congreso de la República de Guatemala existe ya al menos un Proyecto Ley de Habeas Data, el cual tristemente ha quedado en eso, solo un proyecto. Surgiendo la necesidad de retomar el tema, dentro del Organismo Legislativo, pues si aún no se aprueba una ley de protección de Datos Personales, menos aún se tiene en la agenda un proyecto antis pam.

Es importante volver al tema de la protección de datos personales de los guatemaltecos y proponer a la vez una norma que tienda a combatir al spam. Esto tomando en cuenta, que nuestro país ha tenido un avance en los aspectos culturales, educacionales y sobre todo económicos y que lucha a diario por ingresar en los estándares de la economía global, misma en donde se demanda apertura en aplicación de legislaciones modernas que incluyan los hechos ilícitos que han surgido en los últimos tiempos generados por las nuevas tecnologías.



Estas normas jurídicas que se proponen ya no son solo un capricho de estudiante, sino más bien se presenta como una propuesta para darle salidas concretas a casos ya reales a nivel mundial y sobre todo a nivel nacional, que no se pueden dejar a un lado en nuestro país; para el desarrollo económico y social en el que se quiere situar, es por ende, necesario abrir la mente a nuevos cambios nos solo sociales, sino lo más importantes percibirlos en el Derecho.

En Guatemala, debiera de tomarse en consideración para poder legislar a favor del anti spam, lo que el señor Bill Gates (magnate de las telecomunicaciones a través de la internet) comenta: “la lucha anti spam llevará años”. Al magnate que encabeza Microsoft le preocupa “el robo de datos” y sueña con que se termine “la desconfianza” en la comunicación mundial. A pesar de los progresos en la lucha contra el spam, Bill Gates, el hombre más rico del mundo y fundador del gigante informático Microsoft, sabe que esa forma de aprovechamiento publicitario no va poder ser extinguida fácilmente y tiene conciencia que el desafío más inmediato se relaciona con la seguridad. Aún tendremos que luchar con él unos años. Pero en ese terreno concreto ya se han introducido muchas mejoras”, sostuvo refiriéndose al spam, en una entrevista realizada por la revista alemana Der Spiegel, reproducida por el diario El País. Sin embargo, para Gates, la mayoría de los problemas se dan en el “ámbito del robo de datos” y otros aspectos de la seguridad informática, que adquirieron mayor relieve en el auge de la lucha contra el terrorismo desde 2001. El desafío, para el magnate, es lo que la gente se pregunta ahora: “¿Cómo evitar que alguien me robe el número de mi tarjeta de crédito por la Red?”. En ese sentido, advirtió: “Hay ámbitos en que los chicos malos son muy listos, y a veces, más refinados de lo que nos imaginamos”. Gates reveló que hoy, una de sus ambiciones, es poder lograr “poder comunicarnos unos con otros a escala mundial sin desconfianza, y, en consecuencia, de manera más efectiva y creativa”.

Actualmente se están negociando diversos tratados de libre comercio en la Unión Europea y uno de los requisitos que plantea la comunidad europea, es que exista legislación positiva y vigente en relación a ciertos estándares de protección a los datos personales, como se ha intentado advertir, la Ley guatemalteca, no es vanguardista, y en lo que refiere al spam menos, ya que no está en condiciones de garantizar a los



titulares de datos prácticamente ninguna protección.

Es momento de que ya exista una legislación específica en cuanto a la seguridad informática, en especial relacionada a combatir el spam o los correos electrónicos no solicitados o no deseados, en nuestro país, pues como se apuntó no tenemos ninguna legislación al respecto.

3.4. Legislación vigente a nivel internacional enfocada a los correos electrónicos no deseados o no solicitados spam

Efectivamente el problema del spam, por la propia naturaleza de internet y la evolución tecnológica de los medios a través de los cuales se produce, es un problema eminentemente internacional frente al que hay que actuar con medidas de participación internacional, sincronizadas y adoptadas conjuntamente por todos los implicados, de acuerdo con todas las legislaciones, que en ocasiones no regulan esta materia de una misma forma. Para la consecución de esta cooperación internacional se han firmado varios documentos de colaboración y asistencia recíproca con las instituciones que tienen encomendada esa función de supervisión en diferentes países, tanto a nivel comunitario como extracomunitario.

Estos acuerdos firmados, surgen de la necesidad de que actualmente el correo basura o spam, es el azote del correo electrónico y los grupos de noticias en la internet. Los cuales interfieren seriamente con la operación de servicios públicos, por no mencionar el efecto que puede tener en los sistemas de correo electrónico de cualquier individuo. Los spammers están, de forma efectiva, sustrayendo recursos de los usuarios y proveedores de servicio sin compensación y sin autorización.

Como menciona Vint Cerf, Vice President, MCI (empresa de telecomunicaciones por internet) y conocido como "Padre de la internet"; el e-mail (correo electrónico) comercial no solicitado, o abuso de correo electrónico, conocido más comúnmente como "spam," es un problema creciente en la internet. Cualquiera de haya usado la internet por una cierta cantidad de tiempo, probablemente haya recibido solicitudes vía e-mail

para comprar productos y servicios. Y no es tan simple como hacer click en la tecla "Eliminar". El correo electrónico basura mueve el costo del anuncio del anunciante al receptor. Con una simple cuenta de correo electrónico, un spammer puede enviar un mensaje a millones de receptores, convirtiendo tal mensaje en cientos, incluso miles de Megabytes (espacio en nuestro equipo de computo) de datos.⁶

Mencionamos a continuación, algunos de los países en donde ya se cuenta con algún tipo de norma relacionada al tratamiento de datos personales, en especial la protección al dato sensible de la dirección de correo electrónico:

Legislaciones en América de Sur:

1. Argentina: Ley 23.326 de Protección de Datos Personales (Habeas Data, que tiene su fundamento en el Artículo 43 de la Constitución) Incluye sanciones administrativas y penales de carácter pecuniario y se privación de libertad. Existen iniciativas específicas de regulación anti spam en debate, las cuales se basan ya en antecedentes de acciones judiciales.
2. Bolivia: En el Artículo 20 Constitucional, relacionado a la privacidad de las comunicaciones, y los Artículos 363 y 363 constitucionales referentes a la protección de datos. Contempla sanciones pecuniarias y privativas de la libertad bajo la ley penal.
3. Brasil: Artículo 5º Constitucional y la Ley 9.507 la cual regula el derecho de acceso a informaciones y procedimiento de Habeas Data. Existe un Proyecto Ley anti spam, en el Senado del año 2003.
4. Colombia: dentro de las modificaciones constitucionales del año 1991, en el Artículo 15 constitucional. Y dentro de la Ley 527 de 1999 referente a la teletransmisión de datos. Existe actualmente en debate un proyecto ley anti spam.

⁶ "<http://www.cauce.org/problem.html>"

5. Chile: Ley de protección sobre la vida privada, Ley 19.496 y 19.628. Contempla indemnizaciones por daños patrimonial y moral. Ya existen precedentes de acciones judiciales.
6. Ecuador: Ley de Protección a la privacidad y protección de Datos en protección al consumidor y al usuario. Arts. 23.8, 23.13, 23.24 y 94 Constitucional. Ley de Control Constitucional Art. 34. Ley Telecom, Arts 14 y 39. Código Penal en sus Arts. 58 y 64 incluye sanciones por la violación a la intimidad. En la actualidad se trabajan iniciativas de reformas a la Ley de comercio electrónico, firmas electrónicas y mensajes de datos.
7. Guyana: Ley de Protección de datos de Administración Pública. Ley de Telecomunicaciones, Artículos 33, 34 y 35 relacionados al uso indebido de los sitios de comunicación.
8. Guyana Francesa: Legislación aplicable de Francia y UE
9. Islas malvinas e Isla Georgia del Sur: Legislación aplicable de Reino Unido y UE
10. Paraguay: Arts. 33, 36 y 135 Constitución, relacionados a la protección de datos.
11. Perú: Arts. 2, 162 y 200-3 Constitución. Ley que regula el correo electrónico no solicitado (spam), ley específica que regula solo correos electrónicos, incluye sanciones pecuniarias.
12. Uruguay: Ley de Protección de Datos 17.838 del 24-sept-04
13. Venezuela: Ley de Protección al consumidor y al usuario arts. 37 y 38 Privacidad y selección de información. Decreto sobre mensajes de datos y firmas electrónicas Art. 5 sometimiento de mensajes a privacidad de comunicaciones y acceso a la información personal. Ley Especial sobre Delitos Informáticos Arts. 6, 7, 9,

11, 12, 14, 20, 21, 22 Acceso Indebido, daño a sistemas, Espionaje informático, falsificación documentos, Fraude, Violación privacidad de comunicaciones, datos o información personal. Se incluyen sanciones por delitos informáticos de prisión y multas

Legislación en Norte América

1. Alaska: Alaska Statutes Comercio Sección 45.50.479 Limitación en correo electrónico, julio 2003. Regula en relación a la prohibición de envío, etiquetado, y protege el contenido del mensaje comercial
2. Canada: Competition Act Personal Information Protection and Electronic Documents Act Criminal Code of Canada, regula la protección de la información personal. Se requiere previa autorización del individuo para recolectar, usar o difundir su información personal. Deber de proteger la información personal de acuerdo a su grado de sensibilidad derecho de los usuarios a conocer la información que se tiene de ellos y solicitar su corrección.
3. Estados Unidos de Norte América: Can Spam Act, norma directamente por envío spam masivos. En este país, se han organizado y se ha creado CAUCE que es un grupo de usuarios de internet que están ya muy molestos por el spam y han formado una coalición para promover legislación anti spam. Logrando ya un buen trabajo con enmiendas a leyes americanas cuyo origen estaba en miembros de CAUCE. Los fundadores de CAUCE son desde hace mucho tiempo, -- "ciudadanos de internet" reales -- que comprenden el poder de este medio y los peligros del abuso masivo e incontrolado de la internet.
4. México: Ley Federal de Protección al Consumidor. Sanciones no determinadas. Actualmente existen Iniciativa de Ley que regula el correo electrónico. Iniciativa de Ley que reforma y adiciona diversas disposiciones de la Ley Federal de protección al consumidor, Código Penal Federal y Ley Federal de Telecomunicaciones. Iniciativa de



Ley de protección de datos personales. Iniciativas en discusión para delitos cibernéticos

El envío de mensajes no solicitados ha pasado a ser una actividad que reviste un carácter cada vez más delictivo. La legislación puede servir para combatir este flagelo sólo si se aplican sanciones eficaces en caso de incumplimiento. Hasta ahora las sanciones previstas en la mayor parte de la legislación contra este tipo de correo son demasiado moderadas para inquietar a sus autores. En la mayoría de los casos, incluso si finalmente se identifica a los autores de esos envíos, no reciben más que una reprimenda y pueden seguir conservando el producto de sus actividades.

Se tiene de ejemplo a Australia como uno de los países que ha logrado combatir con buenos resultados el envío de estos mensajes. La legislación australiana contra el correo basura da buenos resultados porque impone una multa de 1.100.000 USD (probablemente un riesgo demasiado alto para que los autores de este tipo de mensajes se atrevan a correrlo) y porque el organismo regulador de las comunicaciones de Australia se ha propuesto hacerla respetar.

Ya en la actualidad, la cooperación internacional en la lucha contra el envío de correo no solicitado persigue dos objetivos principales: fomentar la adopción de una legislación eficaz y de normas comunes en los países que aún no las tienen y alentar a los países a cooperar entre sí para hacer respetar eficazmente las reglas aplicables. Aunque en los últimos años se han adoptado numerosas iniciativas, no se dispone todavía de un marco internacional multilateral y coordinado.

El enfoque en cinco puntos definido en la Reunión Temática sobre la lucha contra el correo basura organizada en julio de 2004 por la Unión Internacional de Telecomunicaciones –UIT-, en la misma se plantea la aplicación de una legislación sólida; la adopción de medidas técnicas; el establecimiento de acuerdos de asociación privados (en especial con los proveedores de servicios internet, los operadores móviles y las asociaciones de marketing directo); la sensibilización de los consumidores y los

agentes de la industria con respecto a las medidas “anti-spam” y las prácticas en materia de seguridad de internet, sin olvidar la cooperación internacional a nivel de los gobiernos, del sector de la industria, de los consumidores, de las empresas privadas y de los grupos que combaten este tipo de correo.

Existe mucho por hacer para mejorar la cooperación internacional en la lucha contra este tipo de envíos. En otras palabras, al nivel más simple, esto implica intercambiar información sobre las numerosas y diversas actividades que se realizan. Además, hay que tratar de racionalizar las actividades en el marco de proyectos de cooperación mixta. Un cierto número de iniciativas de cooperación internacional están en curso. El Sector de Normalización de las Telecomunicaciones de la UIT ha adoptado dos Resoluciones al respecto en la Asamblea Mundial de Normalización de las Telecomunicaciones, celebrada en Brasil en 2004 (Resolución 51 — Lucha contra el correo basura (“spam”) y Resolución 52 — Medios técnicos contra el correo basura), cuya aplicación está actualmente en vigor.

A nivel internacional, la Organización de Cooperación Económica Asia-Pacífico (APEC), la Organización de Cooperación y Desarrollo Económicos (OECD) y la UIT están comenzando a reflexionar, en el marco de una serie de reuniones, sobre la manera en que podrían racionalizar los recursos cuyo compromiso han asumido, intercambiando información sobre sus actividades, y contribuir de esa forma a elaborar un programa común para luchar contra el “spam”. Las iniciativas nacionales y regionales encaminadas a sensibilizar a los usuarios acerca de una utilización más segura de internet son cada vez más numerosas. El aumento rápido y reciente de la utilización de datos fraudulentos y la usurpación de identidad, que ha tenido una amplia divulgación en los medios de comunicación, también ha permitido sensibilizar a los usuarios acerca de este problema.

Una nueva iniciativa europea común llamada Red de contacto de las autoridades encargadas del cumplimiento de la legislación contra el correo basura (CNSA) ha sido formulada para combatir este tipo de envíos intercambiando información e iniciando



procedimientos de reclamación transfronterizos en un contexto europeo.

En el caso europeo la solución ha pasado por una mezcla entre una cultura fuertemente comprometida con la privacidad y un conjunto de leyes que sanciona vigorosamente la práctica. En el caso estadounidense la situación es algo más compleja. Por una parte no existe una cultura de la privacidad similar a la europea que permita confiar en los esfuerzos autorregulatorios del sector empresarial. Y si existe no se encuentra suficientemente institucionalizada. Como resulta bien sabido, en los Estados Unidos el tema de la protección de la privacidad ha sido dejado a cargo de los esfuerzos autorregulatorios del mercado. En el caso europeo, en cambio, la protección de la privacidad se encuentra fuertemente regulado.⁷ Junto a lo anterior, en Estados Unidos no existe a la fecha una regulación federal que condene el spam.

A diferencia en la Unión Europea, la protección de los datos personales en el caso de algunos miembros procede con holgura al spam; pero es un número considerable de sus miembros los que ha promulgado una legislación protegiendo la violación al derecho a la privacidad de los sujetos resultante del tratamiento de información personal.

Como se ha anotado, la situación europea es distinta de lo que acontece en el escenario estadounidense; ya que en el primero existe una cierta cultura de privacidad que contribuye decididamente a disuadir la práctica masiva de spam. Europa posee una intensa cultura de protección de datos personales de la cual se encuentra impregnada la industria de ventas a la distancia tradicional. Todos los estados miembros poseen una ley general de protección de datos y una autoridad supervisora, la cual, en algunos casos, ha estado funcionando durante muchos años.

A nivel Europeo, mencionamos a la Agencia Española de Protección de Datos –AEPD– tiene entre sus misiones la defensa de la privacidad de los usuarios de internet frente al spam.

⁷ DE LA MAZA Iñigo: Privacidad y comercio electrónico. 2003



Según datos de la AEPD el spam representa en la actualidad alrededor del 70 % del tráfico mundial de correo electrónico. La AEPD es la autoridad de control independiente que vela por el cumplimiento de la normativa sobre protección de datos. La entrada en vigor de normas en materia de Telecomunicaciones y Servicios de la Sociedad de la Información atribuyen a la Agencia la tutela de los derechos y garantías de abonados y usuarios en el ámbito de las comunicaciones electrónicas. Entre ellas, la defensa de la privacidad de los usuarios de internet frente al spam.

Con esto, en España es posible denunciar el spam, ante la Agencia Española de Protección de Datos, ya que es la competente para perseguirlo, pero en caso que el spam sea de origen español. Esta práctica está sancionada en el artículo 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico que señala:

Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.

a. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.

b. 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 toma de los datos como en cada una de las



comunicaciones comerciales que le dirija.

El régimen sancionador de esta norma califica las infracciones por spam:

3. Son infracciones graves:

...c) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.

...4. Son infracciones leves:

d) El envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 y no constituya infracción grave.

También incluye las sanciones siguientes:

Artículo 39. Sanciones.

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

...b) Por la comisión de infracciones graves, multa de 30,001 hasta 150,000 euros.

...c) Por la comisión de infracciones leves, multa de hasta 30,000 euros.

Respecto a la prescripción de las infracciones dispone:

Artículo 45. Prescripción.

Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses, las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.



Así como existe la Agencia Española de Protección de Datos, existen otros organismos homólogos a esta Agencia, que no solo protegen los datos personales, sino mucho de ellos ya cuentan con competencia en la lucha anti spam, y se encuentran en los siguientes países y son:

Austria: Austrian Data Protection Authority
Bélgica: Privacy Protection Commission
Chipre: Office of the Commissioner for Personal Data Protection.
Dinamarca: Danish Consumer Ombudsman
Eslovaquia: Slovak Personal Data Protection
Estonia: Estonian Data Protection Inspectorate
Finlandia: Data Protection Ombudsman
Francia: Commission Nationale de l'informatique et des Libertés (CNIL)
Grecia: Hellenic Data Protection Authority
Hungría: Data Protection and Freedom of Information Commissioner of Hungary
Irlanda: Data Protection Commissioner
Italia: Garante per la protezione dei dati personali
Letonia: Datu valsts inspekcijas
Lituania: Valstybinė duomenų apsaugos inspekcija
Luxemburgo: Commission nationale pour la protection des données
Malta: Data Protection Commissioner
Países Bajos: College bescherming persoonsgegevens
Polonia: Inspector General for the Protection of Personal Data
Portugal: Comissão Nacional de Protecção de Dados
República Checa: Office for Personal Data Protection
Suecia: Swedish Data Inspection Board

En el caso de América Latina, tenemos la Ley anti spam peruana recientemente aprobada y vanguardista en su género, que ataca de manera frontal el correo electrónico comercial no solicitado (spam) y menciona que será considerado ilegal, en los siguientes casos:

- a.) Cuando no cumpla con alguno de los requisitos establecidos en el artículo 5° de la Ley.
- b.) Cuando contenga un nombre falso o información falsa que no permita identificar a la persona natural o jurídica que transmite el mensaje.
- c.) Cuando contenga información falsa o engañosa en el campo del "asunto" (o subject), que no coincida con el contenido del mensaje.
- d.) Cuando el correo no solicitado se envíe o transmita a un receptor que haya pedido expresamente que no se le envíe dicha publicidad. (después de 2 días de formulado el pedido, el emisor del correo electrónico no debe volver a enviarle nada).

Por ser una ley vanguardista en su género como se apunto anteriormente, se considera de importancia para la visualización de lo que acontece en nuestro continente en relación al spam, la transcripción de la Ley Peruana Anti spam, la cual es:

Ley N° 28493

El Presidente de la República del Perú

Por cuanto:

El Congreso de la República ha dado la ley siguiente:

Ley que regula el uso del correo electrónico comercial no solicitado (SPAM)

ART. 1°— Objeto de la ley. La presente ley regula el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.

ART. 2°— Definiciones. Para efectos de la presente ley se entiende por:

a) Correo electrónico: Todo mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión entre computadoras o cualquier otro equipo de tecnología similar. También se considera correo electrónico la información contenida en forma de remisión o anexo accesible mediante enlace electrónico directo contenido dentro del correo electrónico.



b) Correo electrónico comercial: Todo correo electrónico que contenga información comercial publicitaria o promocional de bienes y servicios de una empresa, organización, persona o cualquier otra con fines lucrativos.

c) Proveedor del servicio de correo electrónico: Toda persona natural o jurídica que provea el servicio de correo electrónico y que actúa como intermediario en el envío o recepción del mismo.

d) Dirección de correo electrónico: Serie de caracteres utilizado para identificar el origen o el destino de un correo electrónico.

ART. 3°— Derechos de los usuarios. Son derechos de los usuarios de correo electrónico:

a) Rechazar o no la recepción de correos electrónicos comerciales.

b) Revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión del servicio de correo electrónico.

c) Que su proveedor de servicio de correo electrónico cuente con sistemas o programas que filtren los correos electrónicos no solicitados.

ART. 4°— Obligaciones del proveedor. Los proveedores de servicio de correo electrónico domiciliados en el país están obligados a contar con sistemas o programas de bloqueo y/o filtro para la recepción o la transmisión que se efectúe a través de su servidor, de los correos electrónicos no solicitados por el usuario.

ART. 5°— Correo electrónico comercial no solicitado. Todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el país, debe contener:

a) La palabra “publicidad”, en el campo del “asunto” (o subject) del mensaje.

b) Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.

c) La inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos basados en internet que permita al receptor manifestar su voluntad de no recibir mensajes adicionales.

ART. 6°— Correo electrónico comercial no solicitado considerando ilegal. El correo electrónico comercial no solicitado será considerado ilegal en los siguientes casos:

a) Cuando no cumpla con alguno de los requisitos establecidos en el artículo 5° de la



presente ley.

b) Contenga nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que transmite el mensaje.

c) Contenga información falsa o engañosa en el campo del “asunto” (o subject), que no coincida con el contenido del mensaje.

d) Se envíe o transmita a un receptor que haya formulado el pedido para que no se envíe dicha publicidad, luego del plazo de dos (2) días.

ART. 7°— Responsabilidad. Se considerarán responsables de las infracciones establecidas en el artículo 6° de la presente ley y deberán compensar al receptor de la comunicación:

1. Toda persona que envíe correos electrónicos no solicitados conteniendo publicidad comercial.
2. Las empresas o personas beneficiarias de manera directa con la publicidad difundida.
3. Los intermediarios de correos electrónicos no solicitados, tales como los proveedores de servicios de correos electrónicos.

ART. 8°— Derecho a compensación pecuniaria. El receptor de correo electrónico ilegal podrá accionar por la vía del proceso sumarísimo contra la persona que lo haya enviado, a fin de obtener una compensación pecuniaria, la cual será equivalente al uno por ciento (1%) de la Unidad Impositiva Tributaria por cada uno de los mensajes de correo electrónico transmitidos en contravención de la presente ley, con un máximo de dos (2) Unidades Impositivas Tributarias.

ART. 9°— Autoridad competente. El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - Indecopi, a través de la Comisión de Protección al Consumidor y de la Comisión de Represión de la Competencia Desleal, será la autoridad competente para conocer las infracciones contempladas en el artículo 6° de la presente ley; cuyas multas se fijarán de acuerdo a lo establecido en el Decreto Legislativo N° 716, Ley de Protección al Consumidor, o en el Decreto Legislativo N° 691, normas de la publicidad en defensa del consumidor, según corresponda.

ART. 10— Reglamento. El Poder Ejecutivo mediante decreto supremo, refrendado por el Ministro de Transportes y Comunicaciones, reglamentará la presente ley en un plazo



máximo de noventa (90) días desde su vigencia.

ART. 11— Vigencia. La presente ley entrará en vigencia a los noventa (90) días de su publicación en el Diario Oficial “El Peruano”.

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los dieciocho días del mes de marzo del dos mil cinco.

Antero Flores-Araoz E.

Presidente del Congreso de la República

Judith De La Mata Fernández

Segunda Vicepresidenta del Congreso de la República

Al señor Presidente Constitucional de la República

Por tanto:

Mando se publique y cumpla.

Dado en la Casa de Gobierno, en Lima, a los once días del mes de abril del año dos mil cinco.

Alejandro Toledo

Presidente Constitucional de la República

Carlos Ferrero

Presidente del Consejo de Ministros

Documento publicado en el Diario Oficial El Peruano el 12 de abril del 2005 “

3.5. Análisis de caso concreto sobre sentencia en contra del spam en la legislación colombiana.

Como caso concreto de lo que actualmente sucede a nivel internacional presentamos el siguiente proceso ejecutado en Colombia, por ser un país latinoamericano, en donde ya no solo se tiene como base el problema del spam o correos electrónicos no solicitados o no deseados, sino además ya existe legislación vigente positiva y como resultado de tal legislación, la sentencia siguiente, la cual transcribimos en sus partes conducentes, por su importancia para el presente trabajo, así:



“República de Colombia
Rama Jurisdiccional del Poder Público
Juzgado Segundo Promiscuo Municipal
Rovira Tolima
Julio veintiuno (21) de dos mil tres (2003)
Rad. 73-624-40-89-002-2003-053-00

Procede esta instancia constitucional a proferir la sentencia que en derecho corresponda dentro de la presente acción de tutela, instaurada por el ciudadano Juan Carlos Samper Posada en contra de Jaime Tapias, Hector Cediell y otros, no encontrando el despacho causal alguna de nulidad que pueda invalidar lo actuado.

Situación fáctica procesal

1. La narra el apoderado de la parte actora en los siguientes términos:

1.1 Juan Carlos Samper es titular del correo electrónico jcsamper@inetwork.com y de todos los demás correos creados bajo el nombre de dominio “i-network.com”.

1.2 Jaime Tapias es una persona natural que actúa bajo el nombre comercial de Virtual Card,

1.3 Virtual Card ofrece los servicios de mailing, multimedia, bases de datos, boletines electrónicos y consultorías e-business a través de internet.

1.4 El 21 de Julio de 2002, Juan Carlos Samper recibió el primer correo electrónico no solicitado de la firma Virtual Card.

1.5 A este correo, Juan Carlos Samper respondió solicitando que fuera retirado de la lista de la base de datos de Virtual Card, ya que no había informado su correo a ninguna base de datos ni lista de correos.

1.6 El 21 de Julio de 2002 a las 20:31, Jaime Tapias, respondió a la solicitud de Juan Carlos Samper lo siguiente: i) que Juan Carlos Samper se encontraba fuera de la lista de Virtual Card, ii) que en mercadeo es permitido buscar prospectos de clientes por todos los medios de comunicación, incluido internet y, iii) que no conocía ninguna legislación sobre privacidad que pudiera limitar la actividad desarrollada por su empresa.

1.7 El 22 de Julio de 2002, Juan Carlos Samper reitera su solicitud de ser retirado de la lista de correo y aclara que el problema radica en que la estrategia de mercadeo se

realice sin solicitud ni autorización de los usuarios.

1.8 A pesar de que Jaime Tapias le había asegurado a Juan Carlos Samper en la comunicación enviada el 21 de Julio que se encontraba fuera de la lista de Virtual Card, el 2 de Septiembre de 2002, Juan Carlos Samper recibió un nuevo correo de Virtual Card en el que le –recordaban- los beneficios del correo electrónico como estrategia de marketing.

1.9 El 3 de Septiembre de 2002, Juan Carlos Samper envió dos mensajes a Virtual Card, en los que solicita una vez más que sus correos sean retirados de la lista de correos. Señala además que ya ha intentado eliminarse de todas las formas posibles

1.10 Un mes después, el 3 de Octubre de 2002, Juan Carlos Samper recibió un correo firmado por Hector Cediell y Consuelo Moreno en el que le anunciaban la alianza estratégica de Virtual Card, Okson Group y Hector Cediell y le solicitaban su autorización para enviar sus promociones a su dirección mail.

1.11 Juan Carlos Samper contestó el 3 de octubre con un contundente -por enésima esima vez saqueme de su lista...-

1.12 El 5 de Octubre de 2002, luego de recibir un nuevo correo de Time Seminarios, cliente de Virtual Card, Juan Carlos Samper intenta una vez más ser retirado de la lista.

1.13 Ese mismo día Time Seminarios le responde que en efecto ha sido retirado de la lista.

1.14 Todos los intentos anteriormente descritos resultaron fallidos. El 18 de Octubre de 2002, Juan Carlos Samper recibió un nuevo correo de la Corporación Innovar, otro cliente de Virtual Card.

1.15 El 19 de Octubre de 2002, Jaime Tapias, envió un nuevo correo a Juan Carlos Samper en el que señala que sabe que su forma de trabajo no es del agrado de Juan Carlos Samper. Agrega que la base general se dejará de usar desde noviembre de 2002 en la cual ustedes se encuentran y luego señala creo que es hora de cambiar el método de esperar un permiso de una persona que nunca lo va a suministrar por el problema del spam y el junkmail opt in. Y concluye su correo con la siguiente frase Señor Samper no es por consolarlo pero a mi correo virtual card me llegan 150 correos publicitarios, porno, basura, virus, etc. que filtramos en el servidor únicamente por colocar la dirección en un directorio de empresas de publicidad.



1.16 Por un tiempo pareció que Virtual Card esta vez había cumplido su promesa. Sin embargo, el 2 de Diciembre de 2002, Juan Carlos Samper recibió un nuevo correo de Lamy, cliente de Virtual Card,

1.17 Finalmente, el 27 de Mayo de 2003, Héctor Cediél, quien se identifica como el encargado de la base de datos, envió un nuevo correo a Juan Carlos Samper.

1.18 En resumen, los demandados y sus clientes, en conjunto, han enviado por lo menos ocho correos electrónicos a Juan Carlos Samper, y éste a su vez les ha enviado por lo menos siete correos electrónicos suplicando de todas las maneras, ser eliminado de la base de datos de Virtual Card.

La presente acción de tutela fue remitida al Juzgado Promiscuo Municipal Reparto, por correo electrónico oficial (adiazg@cendoj.ramajudicial.gov.co) por el accionante Juan Carlos Samper posada representado por apoderado judicial dr., Alvaro Ramirez Bonilla, poder presentado virtualmente ante el Señor Notario Diecinueve del Círculo de Bogota (info@notaria19.com) Dr. Norberto Salamanca F. quien da fe del contenido del mensaje/poder otorgado, acción que fuera repartida extraordinariamente en soporte electrónico, correspondiéndole al Juzgado Segundo Promiscuo Municipal su trámite. Mediante auto de fecha julio ocho de dos mil tres se admitió la solicitud de tutela y se corrió traslado a los accionados Jaime Tapias, Hector Cediél y otros, a su domicilio virtual por medio electrónico (Hcediel@virtualcard.d2g.com; jtapias@virtualcard.d2g.com; irtualcard@007mundo.com y jaime@virtualcard.dns2go.com para que dentro del término de tres (3) días dieran contestación, todo lo anterior con base a los preceptos del artículo 12 de la ley 794 de 2003, que modificó el artículo 107 del Código de Procedimiento Civil, en donde se permite a los Despachos Judiciales hacer uso de las nuevas tecnologías Resúmenes de las contestaciones.

1. Contestación del ciudadano Jaime Leonardo Tapias González

Manifiesta el accionado que la competencia para conocer de la acción de tutela recae sobre los jueces donde ha ocurrido la violación o la amenaza que motivan la solicitud en primera instancia sea contra autoridad pública o particular y por consiguiente no es el Juez promiscuo municipal de Rovira el competente para conocer y fallar la presente



tutela ya que los hechos no ocurrieron en este Municipio. Argumenta que el factor territorial es el elemento principal para que se conozca o no de la acción y que los hechos denunciados ocurrieron en la ciudad de Bogotá por lo cual sería éste el territorio donde se debió instaurar la acción de tutela pues ha sido desde esa ciudad donde se han enviado los correos electrónicos y donde el señor Samper supuestamente recibió los agravios. Igualmente, agrega no estar de acuerdo con lo plasmado en el auto que admitió la tutela pues dice que la tesis plasmada por el señor Juez no tiene un respaldo legal, doctrinario ni jurisprudencial, pero que sí es aplicable para casos en que las comunicaciones puedan enviarse desde cualquier parte y para un usuario que supuestamente no se tiene conocimiento en donde se encuentra pero que en el presente evento se tiene conocimiento el lugar donde se produjo y donde se recibió el supuesto agravio. Sigue argumentando el accionado que el accionante ha escogido este Despacho judicial en forma deliberada pudiéndolo hacer en la ciudad de Bogotá donde funcionan cerca de ciento cincuenta (150) Despachos Judiciales competentes para conocer de la misma con competencia funcional y territorial para hacerlo y por consiguiente buscar: Impedimento de ejercer el Derecho de defensa. Precisamente, ante la distancia existente y la dificultad de comunicaciones no se puede tener acceso a la totalidad del libelo de tutela. Vulneración del Debido proceso. Este aspecto manifiesta que todas y cada una de las pruebas se solicitan a entidades destacadas en esta ciudad o al suscrito en la misma ciudad de Bogotá. Por lo anterior no se puede tener un debido proceso, por no existir la inmediación, porque la práctica de Inspección Judicial, medio idóneo y eficaz para aclarar los supuestos alegados por el accionante y poder determinar que no se ha vulnerado principio fundamental alguno al supuesto ofendido, no se podrá practicar debido a la distancia existente entre el lugar donde funciona este Despacho y la ciudad, de Bogotá donde reposan los diferentes medios de prueba. Respecto de los derechos vulnerados como lo son el de la intimidad y de Habeas Data, estos no han sido violados en ningún momento pues no se encuentran descritos en las sentencias aportadas y que por el contrario con estas sentencias se está explicando que estos derechos no han sido coartados pues ninguno de los textos enviados por él se ajustan a la descripción realizada por la Corte Constitucional y por el Congresista que defiende una ley relacionada con delitos y situaciones informáticos, luego no

entiende de donde se pueda generar la vulneración del derecho fundamental a la intimidad. Respecto de la violación del Habeas data manifiesta que solo posee una dirección electrónica del señor Juan Carlos Samper, y no tiene almacenado algún dato personal. Es mas que inicialmente no conocía el nombre de la persona que mantenía este correo, menos aún su actividad, lugar de residencia y cuales sus ocupaciones. Argumenta el accionado que luego de cruzar algunas comunicaciones con el señor Samper, su correo electrónico desde finales del año pasado ha sido suprimido de sus bases de datos y en lo corrido del año no ha enviado correos ofreciendo productos. Que si ha sido otra persona en este caso el señor Hector Cediell y quizá otras personas quienes han remitido correos al señor Samper a ellos y solo a ellos corresponde abstenerse de hacerlo como el ya lo hizo desde finales del año 2002. Que en su base de datos solo existía su correo electrónico, el cual puede ubicarse en cualquier seminario en el que el mismo actúe, en bases de datos que se adquieren de otras personas o clientes con fines comerciales, etc., pero que nunca contienen ninguna información personal del supuesto ofendido como tampoco nada que pueda serle negativo en su intimidad. Que no es un hecho cierto que el señor Samper continúe en sus bases de datos ya que para finales de 2002 fue definitivamente retirada esta dirección electrónica de su base de datos y que en sus comunicaciones siempre se da la opción al cliente de marcar si quiere recibir mayor información del producto que se le ofrece o si por el contrario, no quiere recibir mas información y para ello, solo basta dar un clic en la casilla que se escoja. Este corresponde al permiso que se le solicita a la persona. Por lo demás, el usuario puede bloquear o no abrir los correos no deseados o basura que diariamente inundan nuestras direcciones electrónicas, especialmente si las mismas corresponden a Hotmail, cuyos servidores operan en el exterior,. Define el término spam como aquella actividad por la cual se envía información no solicitada a un destinatario específico, sin su consentimiento u aprobación. Este se caracteriza por que no registra el origen donde procede entendiéndose por ello la dirección electrónica Email de origen y se envía a múltiples destinatarios. El sistema de envío de Virtual Card, por el contrario, detalla en sus mensajes la dirección de correo de origen, el asunto, la solicitud de permiso para recibir más información, la opción de salir de la lista de envío y la opción de salir de cualquier lista que se encuentre el usuario que lo



solicita. Todo lo anterior dando cumplimiento a las características mínimas de cumplimiento de los boletines de permiso y las herramientas que debe contener para que el usuario no reciba más información. Por lo anterior considera que no se ha violado el derecho fundamental de habeas data que alega el accionante, por lo que tampoco puede prosperar la acción elevada. Concluye diciendo que hará las averiguaciones correspondientes para verificar la legalidad del correo utilizado para su notificación ante el Consejo Superior de la Judicatura y lo relacionado con la reglamentación o cambio de competencia para que la tutela se tramite fuera de Bogotá.

2. Contestación del ciudadano Héctor Cediel

El despacho por el mismo medio electrónico notificó la acción de tutela al señor Héctor Cediel, correo que según su manifestación escrita abrió el 14 de julio el año en curso y se enteró del contenido de la acción respondiéndola escuetamente de la siguiente manera: dice haber enviado un propuesta como agencia de publicidad buscando nuevos productos por este medio electrónico ya que según él, el e-mail marketing es un medio novedoso y de refuerzo y asegura: “ siempre y cuando no se maneje como SPAM “. Que es de conocimiento del accionante Juan Carlos Samper que al colocar el e-mail en tarjetas comerciales o en eventos empresariales está sometido a recibir comunicaciones en cualquier momento. Argumenta que es totalmente viable por su parte y como publicista profesional utilizar las empresas que poseen los equipos para enviar esta información por esta razón recurrió a Jaime Tapias por la economía del servicio. Por lo tanto considera que no incurrió en ninguna violación de la intimidad al ya mencionado señor Samper por cuanto se trataba solamente de una propuesta comercial y que su mail es utilizado únicamente para recibir propuestas comerciales y que es solo su responsabilidad el envío del paquete promocional. Concluye tomando esta situación como un impase y no como una situación que genere un conflicto judicial.

Consideraciones del despacho:

1. El problema jurídico planteado



Conforme a los antecedentes que se han planteado el problema jurídico planteado impone al despacho determinar si es procedente la tutela contra el particular Jaime Leonardo Tapias y determinar que la tutela es viable procesalmente, si analizada la situación que dio origen a ella deben ampararse o no los derechos fundamentales cuya protección invoca el actor.

2. La competencia del juzgado

Se ha planteado que el juzgado no es competente porque la consumación de la conducta vulneradora del derecho fundamental acaeció en la ciudad de Bogotá y que el lugar de residencia de las partes es ese Distrito Capital. El demandado, algo extraño pues conocedor de las nuevas tecnologías, precisamente porque haciendo uso de ellas se le acusa de vulnerar un derecho fundamental, alega una jurisdicción material, olvidándosele la virtualidad que comprende todas las conductas informáticas con implicaciones jurídicas. Ya sobre el lugar de los efectos que produce la vulneración de un derecho fundamental el Consejo de Estado¹ precisamente estudiando el decreto que el demandado arguye en su contestación, al respecto la Sala Plena de esa Corporación se ha pronunciado al afirmar que el lugar donde se produce la violación o amenaza al derecho fundamental no sólo es aquel donde se despliega la acción o se incurre en la omisión, sino también a donde alcanzan los efectos de tales conductas; si bien es cierto que no habla textualmente sobre los efectos virtuales, tal vez por lo novedoso del tema, no es menos verdad que los efectos jurídicos del manejo inadecuado de las nuevas tecnologías se desplegaron en el ciberespacio en donde está ubicado el domicilio virtual del actor; el hecho que ninguna norma lo establezca hasta este momento no nos impide considerar que este Juzgado como cualquier otro en cualquier parte de la República de Colombia, es el competente para conocer de un asunto de esta naturaleza hasta cuando taxativamente la ley señale lo contrario. Los efectos jurídicos del uso de las nuevas tecnologías y su jurisdicción, considera el Estrado no se deben tomar con una simple subsunción, como lo pretende hacer ver el demandado de ubicarlo materialmente en un circunscripción física y formal como se le ha conocido desde antes que se creara la informática como medio de comunicación. Además la Ley Estatutaria de la Administración de Justicia, contempla el uso de las

nuevas tecnologías al servicio de la administración de justicia, precisamente en su artículo 95, reza que los Juzgados, Tribunales y Corporaciones judiciales podrán utilizar cualesquier medio técnico, electrónico, informático y telemático para el cumplimiento de sus funciones. También dice que los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad y seguridad de los datos de carácter personal que contenga en el término que establezca la ley. Como Juez Constitucional el ámbito jurisdiccional es todo el territorio nacional y la norma no excluye mi competencia en el ciberespacio, porque recordemos de que se está hablando de un hecho ocurrido en este ámbito así el demandado no lo quiera reconocer pese a que se trata de un informático, resultando muy asombroso su actitud de que querer quitarle relevancia al medio en donde precisamente está realizando sus tareas de e-marketing. La competencia, el demandado la está circunscribiendo a unas coordenadas físicas, pero se le ha olvidado que el meollo del asunto es la virtualidad y precisamente el domicilio virtual del señor JUAN CARLOS SAMPER es su correo electrónico, tan seria es esta dirección que nuestra legislación le dio amparo cuando obliga a los comerciantes a registrar su domicilio virtual en la cámara de comercio en donde aparecen asociados, tal es el caso del artículo 29, parágrafo único de la Ley 794 de 2003. Sobre la competencia virtual, pese a que somos pocos los colombianos que lo exponemos, existen varios tratadistas latinoamericanos que hablan sobre el domicilio, entre otros, el Maestro Julio Núñez Ponce que afirma que el tema de domicilio virtual está directamente relacionado con el tema de jurisdicción y competencia en internet y que los comentarios efectuados a normas existentes a su ordenamiento jurídico (Perú) le permiten aproximarse al contenido que podría darse al domicilio virtual en sus implicaciones civiles, societarias y tributarias, esto es, que el domicilio material de un ciudadano se le toma como el de la dirección (o lugar) de la ciudad en donde habita ora en donde desarrolla sus actividades profesionales, igualmente pasa con la dirección del correo electrónico, es allí en donde desarrolla diferentes actividades virtuales las que puede realizar en cualquier parte del mundo, siendo éste su domicilio virtual que jamás debe ser asimilado en forma exacta con la materialidad de otros domicilios. El Domicilio Virtual estaría conformado por la dirección electrónica que constituye la residencia



permanente en la Web de la persona. Pensemos que el domicilio ordinario de un ciudadano común lo constituye la residencia habitual que tiene en un lugar, lo que implicaría en tratándose de su domicilio virtual, la utilización constante de una dirección electrónica, la que puede ser su home page su e-mail, como lo son actualmente los comerciantes y personas jurídicas⁶ inscritos en el registro mercantil, porque deben registrar su e-mail pop3 o smtp⁷ ora el de su Homs page que es otra forma de notificación virtual, ya en otrora oportunidad este Estrado notificó a Ministros del Despacho de la Administración del Dr. Andrés Pastrana, por acción de tutela que se inició para ese entonces en contra de la Nación, accediendo a su página virtual; lugar en donde se le enviarían las notificaciones informáticas; algo igual acontecería, con las personas jurídicas o comerciantes para la ejecución de actos jurídicos electrónicos, sobre todo en materia de notificaciones judiciales, comercio electrónico y transferencia de fondos. Por lo plasmado anteriormente, no es de recibo para el Estrado lo referente por el accionado respecto del contenido del auto admisorio de la tutela en donde manifiesta que lo anteriormente esbozado es una simple teoría sin respaldo legal, doctrinario o jurisprudencial, cuando la realidad legal es totalmente diferente, porque el parlamento no solo ha proferido las leyes 5278 de 1999 y 7949 de 2003, que se refieren al uso del dato informático, porque además existen toda una reglamentación que sobre el tópico expiden las diferentes superintendencias del país. Traigo a colación una frase sobre la aterritorialidad de la internet de Johnson y Post: -El ciberespacio no tiene fronteras basadas en el territorio ya que el costo y velocidad de envío de la transmisión de un mensaje en la Red es casi completamente independiente de la ubicación física: los mensajes pueden ser transmitidos desde cualquier ubicación a cualquier ubicación sin arruinarse. degradarse o demorarse sustancialmente más y sin que ninguna barrera física o que pueda mantener lugares y personas remotamente alejados separados unos de otros-

3. La firma electrónica

El demandado ha argüido que los documentos expedidos por este Estrado en soporte electrónico no tienen ninguna validez en razón a que no están firmados analógicamente y no tiene el amparo de ninguna entidad de certificación de firma digital. Se conoce en



el mundo del Derecho Informático la diferencia entre firma digital y firma electrónica, o Art. 315 Código de Procedimiento Civil, modificado por la Ley 794 de 2003 7 POP Postal Office Protocol: Servidor de correo entrante. SMTP Simple Mail Transfer Protocol: Servidor de correo saliente. Seguramente la presente actuación electrónica generará algunas falencias, por razones propias, tal vez esta pieza procesal se torne en la primera en el país y origina una novedad en el uso de las nuevas tecnologías, pero el Estrado cree que a medida que pase el tiempo el uso de la informática será masivo, cumpliendo así los propósitos del de la descongestión (Despachos al día), economía (no mas soporte papel) y celeridad (rapidez en al información) de las actuaciones judiciales. La firma digital, cuando se implemente en los trámites judiciales, tal vez superemos los escollos que hoy se presentan con el manejo de los documentos en soporte electrónico. Ésta consiste básicamente en la aplicación de algoritmos de encriptación a los datos, de esta forma, sólo serán reconocibles por el destinatario, el cual además podrá comprobar la identidad del remitente, la integridad del documento, la autoría y autenticación, preservando al mismo tiempo la confidencialidad. La seguridad del algoritmo va en relación directa a su tipo, tamaño, tiempo de cifrado y a la no violación del secreto. Ahora bien, este despacho judicial está recibiendo correspondencia continuamente procedente de la oficina de la administración judicial, consejo seccional de la judicatura y otros entes judiciales, a la cual se le da plena credibilidad, por provenir, precisamente de despachos acreditados y confiables, así la correspondencia llegue en fotocopia y sin una firma original; pero lo que se quiere dar a entender es la confiabilidad de su procedencia para así mismo no dudar del contenido; para citar el caso mas reciente tenemos el recibo de la circular No. 47 emanada de la presidencia de la Sala Administrativa del Consejo Superior de la Judicatura en donde el presidente Dr. Gustavo Cuello Iriarte, establece unas directrices para el trámite de las comisiones, comunicación que no viene con rúbrica analógica. Siguiendo el linderio interpretativo del demandado, el Estrado no debería acatar lo ordenado en dicha circular por la potísima razón de no venir firmada. Con ello queremos significar que el método utilizado para el envío de dicho documento, la Dirección de Administración Judicial del Tolima, nos permite identificar el iniciador del mensaje, lo que indica que su contenido cuenta con su aprobación; el método de comunicación se torna confiable y

apropiado para cumplir los propósitos de su contenido. Todo esto se le debe sumar el principio constitucional de la buena fe, que se entiende plasmado en todas las conductas del hombre hasta cuando no se le pruebe lo contrario.

4. La Solución al problema

Considera el Estado de Colombia que desde el punto de vista procesal es procedente la acción de tutela contra el particular Jaime Leonardo Tapias, porque el solicitante con respecto a éste se encuentra en un estado de indefensión.

En relación con el estado de indefensión, recordemos que en el texto constitucional correspondiente al artículo 86, dice que la ley establecerá los casos en que la acción de tutela procede contra particulares respecto de quienes el solicitante se encuentre en estado de subordinación o indefensión. Es importante resaltar entonces que la indefensión se predica respecto del particular contra quien se interpone la acción. Este particular es quien con su conducta activa u omisiva pone en peligro o vulnera un derecho fundamental correcto del indefenso. Además la tutela se torna procedente porque el accionante acreditó cómo en varias oportunidades lo hizo la súplica a los demandados para que no le enviaran mas mensajes no solicitados como también lo borrarán de sus base de datos, porque no había autorizado su difusión y recepción de mensajes. De conformidad con el numeral 4º. Del art. 42 del decreto 2591 de 1991, el estado de indefensión acaece o se manifiesta cuando la persona ofendida por la acción u omisión del particular, sea éste persona jurídica o su representante, se encuentra inerme o desamparado, es decir, sin medios físicos u jurídicos de defensa o con medios y elementos insuficientes para resistir o repeler la agresión o la amenaza de vulneración a su derecho fundamental; estado de indefensión que se debe deducir, mediante el examen por el Juez de la tutela, de los hechos y circunstancias que rodean el caso en concreto. No es otra la situación del accionante puesto que el medio utilizado por el particular tiene el suficiente poder de penetración que no ha podido ser repelido por el agredido a pesar de sus múltiples súplicas para que se deje de bombardear con información no solicitada, lo cual denota la situación de indefensión pues este no parece disponer por sí mismo de una situación de equivalencia que le permita contrarrestar en igualdad de condiciones la sensación adversa generada en su contra.



5. Los presuntos derechos vulnerados

5.1. El medio empleado para vulnerarlos el spam. El apoderado del actor, alega que a su cliente se le vulneraron los derechos de habeas data, autodeterminación informática y el de intimidad, a través de correo spam; antes que analicemos si se han violado o no dichos derechos fundamentales, el Estrado considera necesario entrar a hacer algunas consideraciones sobre lo que es el spam o ACE12, como lo llaman en Europa.

6.2. Los Derechos Fundamentales Vulnerados

6.2.1 La sensibilidad del dato electrónico, la autodeterminación informática, el derecho a la intimidad y habeas data. Actualmente, todos los individuos – voluntariamente - proporcionan sus datos personales a distintas instituciones públicas o privadas, por distintas razones. El apropiado tratamiento de los datos, permite convertirlos en información útil para el logro de determinados objetivos. Pero esos datos pueden amenazar la dignidad de los hombres por el uso arbitrario y malicioso de la informática. El peligro se concreta con la capacidad de almacenamiento en la memoria de los ordenadores, la celeridad de todo el proceso, el desarrollo de las disímiles técnicas reservadas para el manejo de volúmenes de información, etc. El ordenador puede verificar los datos sobre un individuo introducidos en su memoria y cotejar la imagen real de los datos del individuo en cuestión. Todos esos datos deben ser protegidos contra el acceso de quienes no estén autorizados. Esta necesaria protección es un límite al manejo de la informática ante el temor de que pueda atentar la intimidad de los ciudadanos y que pueda restringir el ejercicio de sus derechos. Una base de datos, esta compuesta por todo tipo de información aportados por las personas para determinados fines. Pero también existe una gran variedad de medios a través de los cuales se compila información de las personas sin su consentimiento, tal como sucede en algunos sitios de internet que cruzan datos de las personas que las visitan y conforman un perfil del interesado. La existencia de enormes bases de datos que contienen gran cantidad de información referida a las personas, es una consecuencia de la informática y sin la

cual sería imposible su existencia. Lo importante es la finalidad para el cual se usará la información allí almacenada para evitar que seamos discriminados debido a un uso desatinado de sus datos. La cuestión es aun más grave si especulamos que esas bases de datos pueden ser atacadas por crackers que son aquellos aficionados a la computación que obtienen accesos no autorizados a los sistemas de computación, robando o destruyendo datos, y que buscan información para sí o para terceros. La ambición para conseguir datos no es el mismo que para actualizarlos, rectificarlos, suprimirlos o modificarlos. La doctrina especialista en el tema, se refiere al amparo debido a los ciudadanos contra la posible utilización por terceros de sus datos personales susceptibles de tratamiento automatizado para confeccionar una información que afecte a su entorno personal, social o profesional en los límites de su intimidad. *La protección de datos está prevista por las innovadoras legislaciones mediante el derecho a la intimidad y su transmisión telemática* cuando aparece una nueva relación entre datos y personas que necesitan ser protegidos más allá de las normas referentes a la intimidad. Lo primordial es que los datos no generen situaciones de segregación por cuestiones de salud, raza, ideas, costumbres y datos que pudieran llegar a limitar nuestras posibilidades. Son base de datos privadas los datos que tienen reguladas situaciones o circunstancias en que la persona se ve obligada a darlos o ponerlos en conocimiento de un tercero, debiendo impedir su difusión y respetar la voluntad de secreto sobre ellos, de su titular. A su vez, dentro de los privados encontramos los datos personales íntimos, que son aquellos que el individuo puede proteger su difusión frente a cualquiera y que, de acuerdo con un fin determinado, está obligado a dar, salvo algunas excepciones. Estos datos secretos son los denominados datos sensibles, definidos por la Constitución Nacional en su artículo 15 que en su tenor literal dice: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas" Y como datos personales que requieren una protección especial, tales como ideas políticas, creencias religiosas, salud física o mental, comportamiento sexual de los individuos y la autodeterminación informática. Este es el derecho conocido como habeas data,



considerado hoy como uno de los más importantes derechos fundamentales, especialmente dado el desarrollo de la cibernética, la informática y la telemática y en general de la información y las comunicaciones en la actualidad. En forma errada el demandado constitucional alega que el derecho de habeas data sólo es viable para cuando se refiere a datos financieros, precisamente sobre el tópico el Dr. Nelson Remolina⁸ en conferencia ofrecida en el Hotel Ambalá, en la ciudad de Ibagué, se refería que el habeas data se establece el manejo de cualquier dato sensible, de ahí el porque se torna viable una acción de tutela para cuando, en un centro asistencial se le diagnostica a un paciente erradamente una enfermedad terminal y se publican sus datos. Compartimos la tesis del Dr. Remolina, porque no puede ser excluida en ninguna ley, la viabilidad de la acción de amparo para cuando se manejan datos diferentes a los financieros como los que usualmente manipulan la mayoría de las empresas que conservan bases de este tipo. Podríamos decir que una de las mas frecuentes violaciones de los derechos humanos en el presente la constituyen las actuaciones de entidades particulares o públicas que tienen por objeto recopilar información confidencial o personal de los individuos, sin que el dato sea verificado, ni conocido por la persona afectada por el mismo o ilegalmente manipulado. Igualmente este manejo informático del dato impide la actualización y el olvido con que la persona está sujeta irredimiblemente a soportar la carga de su pasado o de un uso impropio de la información confidencial o de sus registros informáticos, para ser utilizada como medio de presión para alcanzar fines desleales o propósitos ilícitos. Por su parte nuestra Corte Constitucional ya se ha referido al respecto sobre el derecho de la intimidad afirmando que: “Es un derecho entonces, personalísimo, según inspiración constitucional relativa a la dignidad humana, que debe ser tutelado cuando, por la acción de terceros, se produce una intromisión indebida en el ámbito personal o familiar del sujeto que

⁸ Nelson Remolina Angarita. Abogado y especialista en Derecho Comercial de la Universidad de los Andes. Master en Leyes the London School of Economics and Political Sciences, con énfasis en derecho informático y económico (information Technology Law; Electronic Banking Law; International Economic Law; International Trade Law). Director de Pregrado y profesor de la Facultad de Derecho de la Universidad de los Andes. Profesor de postgrados de las Facultades de Ingeniería y Administración de la Universidad de los Andes. Autor de los temas DATA PROTECTION E INFORMATICA EL DOCUMENTO ELECTRÓNICO y DATA PROTECTION Panorama nacional e internacional, publicado en el libro INTERNET COMERCIO ELECTRÓNICO & TELECOMUNICACIONES por la Universidad de los Andes en asocio con Legis. 2002



conlleva la revelación de asuntos privados, el empleo de su imagen o de su nombre, o la perturbación de sus afectos o asuntos más particulares e íntimos relativos a su sexualidad o salud, con o sin divulgación en los medios de comunicación. Se ha considerado doctrinariamente, que constituyen aspectos de la órbita privada, los asuntos circunscritos a las relaciones familiares de la persona, sus costumbres y prácticas sexuales, su salud, su domicilio, sus comunicaciones personales, los espacios limitados y legales para la utilización de datos a nivel informático, las creencias religiosas, los secretos profesionales y en general todo "comportamiento del sujeto que no es conocido por los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación" que éstos tienen de aquel.⁹ ... En nuestro derecho positivo, que posee un rango constitucional, la evolución de este derecho puede resumirse desde el "secreto" al "control" de la información que se tiene de uno mismo en los bancos de datos. Este derecho a la intimidad se encuentra por estos días seriamente amenazado por la capacidad que posee tanto el sector público como el privado, de acumular gran cantidad de información sobre los individuos en forma digital. Con el desarrollo constante e ininterrumpido de la informática y las telecomunicaciones, se permite a tales entidades a manipular, alterar e intercambiar datos personales a gran velocidad y bajo costo. Así obtenemos sociedades altamente informatizadas en la que nuestras conductas y acciones son observadas y registradas y será imposible evitar la estigmatización y encasillamiento. En Colombia se tramita el proyecto de Ley No. 16638 de 2003, el que "Por el cual se regulan las comunicaciones vía internet y mediante el uso de fax " y en lo que se refiere al spam los legisladores consignaron el siguiente tipo: "Artículo 5. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas". Igualmente se consagró una sanción dentro del párrafo único del artículo 3°, que reza: "Párrafo: Cuando por el mal uso del internet o fax se atente contra el patrimonio moral de las personas, se ponga en riesgo su vida o atente contra la seguridad y la estabilidad económica de las empresas, cualquiera que

⁹ Sentencia SU 089 de 1995 del Dr. Jorge Arango Mejía. Sentencia citada por la Corte Constitucional en la T-411 de 13 de Septiembre de 1995. MP. Alejandro Martínez Caballero. 13 de Septiembre de 1995 S. U - 089 de 1995, Colombia.

fuese su actividad, las autoridades competentes pueden, con fundamento en los libros de registro, aplicar a los responsables el rigor de las leyes preexistentes en materia civil, comercial o penal para castigar a dichas personas”. Esteremos atentos del futuro legislativo que atañe la atención de este Despacho en el día de hoy, por lo pronto resulta oportuno acotar que España es de los pocos estados que prohíbe absolutamente esta técnica gracias a dos leyes: LSSICE y LORTAD (la primera regularía la utilización del spam y la segunda el origen de los datos ilícitos sin autorización del propietario), que imponen en ambos casos severas sanciones a los responsables.

6.2.2. La vulneración de los derechos fundamentales

Alega el demandado Jaime Leonardo Tapias González, que se le vulneró el derecho al debido proceso, en razón a la distancia no se practicaron las pruebas que se deberían hacer en la ciudad de Bogotá, y poder probar que no había vulnerado ningún derecho constitucional. Consideramos que dichas pruebas no eran necesarias precisamente por la confesión que el mismo ciudadano demandado hace en su libelo, porque reconoce que sí le ha enviado correspondencia no solicitada al actor del que conservaba la dirección de su correo electrónico en su base de datos. Extrañamente no refiere el ciudadano Tapias tener vinculación alguna con su compañero de demanda, esto es, el señor Héctor Cediél, pese a que éste en el traslado de la demanda constitucional acepta haber contratado los servicios del señor Tapias Gonzalez en el manejo de su e-marketing. El señor Tapias Gonzalez, en toda la extensión de su escrito de traslado, ha intentado derrumbar por todos los medios la competencia del Estrado, pero se despreocupó de desvirtuar los cargos; no aportó prueba alguna que nos indicará que los argumentos del actor no eran verdad, esto es, que desvirtuara los cargos de haber vulnerado los derechos constitucionales del señor Samper, como hubiera sido a guisa de ejemplo, que nos hubiera aportado algún contrato virtual que nos enseñara que contaba con la anuencia de éste para recibir mensajes comerciales, como también de manipular su dirección electrónica, lo que en el medio se llama, e-marketing de permiso, en donde se invita al presunto o potencial cliente a recibir los catálogos de



productos o servicios ofertados virtualmente, de esta manera una vez contando con la aprobación Proyecto de ley No. 166-02 por el cual se regulan las comunicaciones Vía internet y mediante el uso de fax ponente Alvaro Ashton Giraldo Representante a la Cámara Departamento del Atlántico del futuro cliente, se le remitiría hasta cuando el quiera recibir, los mensajes comerciales. Así es como se debe manejar el mercado virtual, con principios éticos. Aquella consigna que se agrega a todo spam de que si no quiere recibir más mensajes comerciales, sólo es remitir al postmaster su deseo de no querer recibirlos, es inconstitucional, puesto que se le pide una exclamación sobre un hecho no consentido. Sabemos que el spam es el envío indiscriminado de mails no solicitados. Si yo recibo un mail que no solicité de una persona que no conozco, y que al mismo tiempo es enviada a una cantidad de personas que tampoco lo solicitaron, eso es spam. No debería tener necesidad de enviar un mail para que me borren de una lista ya que no deberían agregar mi dirección a ninguna de ellas, puesto que no he autorizado a estar incluido, es ahí en donde se me vulnera mi derecho constitucional y continúa la vulneración cuando comienzan a comercializar mi dirección electrónica, que tampoco he autorizado. Esta advertencia sólo se torna viable si el titular de la cuenta de correo electrónico ha autorizado recibir dichos mensajes, como cuando aceptamos recibir noticias o catálogos al cargar un software en nuestros equipos que ha sido bajado de la internet. Además, la mayoría de las veces, al responder el mail pidiendo ser removidos de la lista, lo único que estamos haciendo es confirmar que nuestra dirección existe, con lo cual, en lugar de dejar de recibir mensajes, comenzamos a recibir más. Recibir spam, es como cuando encuentro a un mismo vendedor golpeando insistentemente en mi casa, para ofertarme sus productos que vende, de los cuales no necesito, yo le replico no quiero nada suyo y le suplico a su vez no insistir ya que no me interesa su genero de productos. Nuevamente el mismo señor u otro personaje, me vuelven a ofrecer los mismos productos, los que no me interesan. El Habeas Data brinda el derecho a toda persona de conocer qué datos propios han sido incluidos en registros y bancos de datos o en registros privados, destinados a proveer de informes, para pedir su supresión, rectificación, confidencialidad o actualización en caso de falsedad o discriminación. Los riesgos a los cuáles esta expuesta la vida privada de las personas en la sociedad de la información, en particular, aquellos derivados del

tratamiento de datos personales a consecuencia de la utilización de las nuevas tecnologías de la información y de la comunicación, nos hacen cuestionar cual debe ser el rol del derecho ante la referida problemática. En relación con el derecho a la intimidad, este hace referencia al ámbito personalísimo de cada individuo o familia, es decir, a aquellos fenómenos, comportamientos, datos y situaciones que normalmente están sustraídos a la injerencia o al conocimiento de extraños. Lo íntimo, lo realmente privado y personalísimo de las personas es, como lo ha señalado en múltiples oportunidades la Corte, un derecho fundamental del ser humano, y debe mantener esa condición, es decir, pertenecer a una esfera o a un ámbito reservado, no conocido, no sabido, no promulgado, a menos que los hechos o circunstancias relevantes concernientes a dicha intimidad sean conocidos por terceros por voluntad del titular del derecho a por que han trascendido al dominio de la opinión pública... La Libertad Informática o Autodeterminación Informativa, ha sido denominada por la doctrina española y colombiana como “un nuevo derecho fundamental que tiene por objeto garantizar la facultad de las personas, para conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos y controlar su calidad, lo que implica la posibilidad de corregir o cancelar datos indebidamente procesados y disponer sobre su transmisión”. Esta facultad, es lo que se conoce como Habeas Data que constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática. En el art. 20 de la Constitución Política se garantiza a toda persona la libertad de expresar y difundir sus pensamientos y opiniones, la de informar y recibir información veraz e imparcial, es decir, se trata de una libertad que opera en doble vía, porque de un lado se reconoce la facultad de la libre expresión y difusión de las ideas, conocimientos, juicios u opiniones y de otro se proclama el derecho de acceder o recepcionar una información ajustada a la verdad objetiva y desprovista de toda deformación. En corolario de lo anterior, el Estrado tutelaré los derechos de habeas data, autodeterminación informática y el de intimidad al ciudadano Juan Carlos Samper Posada, por habersele violado en las circunstancias que arriba se anotaron. Por lo anteriormente expuesto, el Juzgado Segundo Promiscuo Municipal de Rovira Tolima, administrando Justicia en nombre de la República de Colombia y por autoridad de la Ley, entre otras sentencia del Consejo de Estado Sala de lo Contencioso



Administrativo sección tercera Consejera ponente: Maria Elena Giraldo Gómez Bogotá D. C., treinta y uno (31) de octubre de dos mil uno (2001) Radicación número: 25000-23-24-000-2001-1338-01(AC-1529) Actor: Amparo Barajas García Referencia: Acción de Tutela. Y de la Corte Constitucional las siguientes, entre otras: T-157/94, T-164/94, T-094/95, T-096A/95, T- 097/95, T-199/95). **FALLA: PRIMERO:** TUTELAR como en efecto se hace los derechos a: habeas data, autodeterminación informática y a la intimidad, del ciudadano Juan Carlos Samper Posada. **SEGUNDO:** ORDENAR a los señores Jaime Leonardo Tapias Gonzalez representante de la firma Virtual Card y a Héctor Cediel, una vez en firme esta providencia no remitir mas correo no solicitado (spam o ace) al señor Juan Carlos Samper Posada a su cuenta de correo electrónico jcsamper@network.com y todos los demás correos creados bajo el nombre de dominio i-network.com. **TERCERO:** ORDENAR a los señores Jaime Leonardo Tapias Gonzalez y Héctor Cediel una vez en firme esta decisión, borrar la dirección de correo electrónico jcsamper@network.com y todos los demás correos creados bajo el nombre de dominio i-network.com, cuyo titular es el ciudadano Juan Carlos Samper Posada, de sus respectivas bases de datos para el manejo de e-marketing en sus empresas. **CUARTO:** Se procede a notificar a los demandados en sus correeos electrónicos (jtapia@virtualcard.d2g.co; jaime@virtualcard.dns2go.com y hcediel@virtualcard.d2g.com) surtiéndose la fórmula señalada en el artículo 29 de la Ley 794 de 2003, que modificó el artículo 315 del Código de Procedimiento Civil. El presente documento electrónico está amparado en los preceptos de los artículos 6°,7° y 8° de la Ley 527/99 que se refiere al mensaje de datos. **QUINTO** Contra la presente decisión procede el recurso de impugnación consagrado en el art. 31 Decreto 2591 de noviembre 19 de 1991.

COPIESE, NOTIFÍQUESE Y CÚMPLASE

ALEXÁNDER DÍAZ GARCÍA

Juez”

Como se ve, con esta sentencia, se sienta un precedente jurisprudencial, en relación a lo negativo que suele suceder con el spam, con esta sentencia, se deja plasmado en el año 1991, lo vanguardista de la legislación colombiana y del actuar de sus jueces. Se

logra que efectivamente el actor, sea amparado y tutelado y se ordene a los demandados a ya no enviar más spam a la cuenta del correo electrónico del actor, correo basura, que no solo llenaba de espacio su equipo, sino además quitaba tiempo, dinero y hacia perder información valiosa.

En la actualidad, se siguen discutiendo nuevas leyes anti spam que contribuyan a la lucha contra el envío masivo de correos electrónicos no deseados o no solicitados, que perjudican a las personas individuales y jurídicas en su patrimonio y su moral.

3.6. Decálogo para prevenir y sancionar el spam, aprobado por la Agencia Española de Protección de Datos

Con motivo de la celebración del Día de internet en España el 25 de octubre, la Agencia Española de Protección de Datos presenta un Decálogo cuyo objetivo es reducir la brecha digital, y reiterar recomendaciones para combatir y prevenir el spam. Dicho decálogo, se transcribe literalmente debido a la relación con el tema tratado y su importancia.

Decálogo para prevenir y sancionar el spam

1. Ser cuidadoso al facilitar la dirección de correo. Facilitar únicamente la dirección de correo a aquellas personas y organizaciones en las que confía y que quiera comunicar.
2. Utilizar dos o más direcciones de correo electrónico. Utilice una dirección para aquellos casos en los que no se confíe o conozca lo suficiente al destinatario, y otra dirección personal que sea conocida únicamente por sus amigos o por sus contactos profesionales.
3. Elegir una dirección de correo poco identificable. Para crear una dirección de correo electrónico y reducir el envío de spam, sería conveniente no introducir campos que sean potencialmente identificables por el spammer.



4. No publicar la dirección de correo. No se debe anunciar la dirección de correo en buscadores, directorios de contactos, foros o páginas Web. Cuando envíe correos en los que aparezcan muchas direcciones, envíelas usando con copia oculta. Si es necesario facilitar la dirección de correo en alguna Web, escriba 'at' o 'arroba' en lugar de @. Asimismo, si reenvía un correo, elimine las direcciones de los anteriores destinatarios.

5. Leer detenidamente las Políticas de Privacidad y las Condiciones de Cancelación. Si se va a suscribir a un servicio on line (en línea) o a contratar un producto, revise la política de privacidad. No dude en ejercer los derechos de acceso y cancelación sobre sus datos ante estas empresas.

6. Sensibilizar a los niños sobre la utilización del correo y la mensajería instantánea. Los niños son objetivos ideales para promocionar información sobre la composición y las prácticas de consumo del hogar. Además, los correos que pueden tener contenidos no aptos para los niños.

7. No es conveniente contestar al spam. Es conveniente desactivar la opción que envía un acuse de recibo al remitente de los mensajes leídos del sistema de correo electrónico. Si un spammer recibe dicho acuse sabrá que la dirección está activa, y lo más probable es que le envíe más spam.

8. No pinche sobre los anuncios de los correos basura. Entrando en las páginas Web de los spammers podemos demostrar que nuestra cuenta de correo está activa, con lo que puede convertirse en un objetivo para nuevos envíos.

9. Utilice filtros de correo. Los programas de gestión de correo electrónico y muchas páginas Web ofrecen la posibilidad de activar filtros que separan el correo deseado del spam.



10. Mantenga al día su sistema. Utilice programas antivirus y actualizaciones y parches que corrigen los problemas detectados en los programas de su equipo. Además, es muy recomendable la instalación de cortafuegos para monitorizar lo que ocurre en el ordenador.



CAPÍTULO IV

4. Propuesta de proyecto de ley anti spam en Guatemala

4.1. Propuesta sobre aspectos que debe contener un proyecto anti spam en nuestro país

Actualmente existe un nutrido conjunto de normas legales que regulan el tratamiento de datos personales y, con diversidad de enfoques y mayor o menor intensidad, el spam. Aún cuando no es posible examinar detalladamente aquí la fisonomía de las distintas regulaciones, trataremos de tomar lo básico y fundamental para poder dar en mínima forma una Propuesta sobre los aspectos clave que debe contener un Proyecto de Ley Anti spam.

Deben considerarse antes que nada cinco opciones al momento de regular el spam:

1. La opción prohibitiva: la cual consiste en proscribir todo tipo de publicidad comercial no consentida. Una versión más popular y genérica señala que consiste en prohibir únicamente el envío de publicidad por correo electrónico cuando esta no haya sido solicitada, es decir, que el receptor haya prestado su consentimiento sobre la recepción de correos- o bien exista una relación anterior entre el emisor y el receptor. La ventaja de este enfoque es evidente, por una parte reduce significativamente el número de correos enviados y, por otra, solo reciben correos quienes los desean.

2. El “etiquetamiento” de spam como spam: el etiquetamiento de los correos comerciales consiste en indicar en el “asunto” (subject) del mensaje su carácter comercial. De esta manera, solo serían permitidos aquellos correos que identificaran con suficiente elocuencia su contenido. Etiquetar correos posee dos ventajas. De una parte permite a los usuarios disminuir el tiempo y recursos que utilizan bajando correos, de otra facilita el funcionamiento de los filtros que utilicen los usuarios para evitar el ingreso de publicidad a sus respectivas casillas.

3. La opción anti-fraude: este enfoque consiste: en sancionar aquellos correos electrónicos masivos cuando utilizan el nombre de dominio de una tercera parte sin su autorización o, de otra manera, disfrazan el verdadero punto de origen del correo electrónico o contienen información falsa o engañosa en la línea del “asunto” del correo electrónico. La importancia de ambos mecanismos es que endosan dos de los problemas más frecuentes en el envío de correos no deseados, a saber la introducción de nombres de dominio falsos o información de enrutamiento (routing) y el despliegue de información engañosa en la línea de asunto del correo electrónico. Este enfoque favorece la regulación de esquemas de “opt-in”, esto significa que solo se permite el envío de publicidad cuando el receptor ha dado su consentimiento explícito para que se le envíe publicidad. Lo anterior puede funcionar a través de inscripciones en sitios web específicos aceptando el envío de publicidad o bien en listas más generales en las que el receptor acepta el envío de publicidad. El problema que esto puede tener, además de los problemas comunes a toda la legislación sobre spam, reside en que es poco probable que la exclusión funcione salvo que se tutele la creación de mecanismos que garanticen la obtención del consentimiento por parte de los receptores.

4. La utilización de bienes muebles sin autorización: alguna legislación basada en un nutrido contingente de casos resueltos por tribunales norteamericanos en los últimos años, ha utilizado esta figura para enfrentar el spam; para que el spammer sea imputable de la utilización no consentida de bienes muebles, quien la alega debe acreditar algún tipo de interferencia sustancial al ejercicio de su dominio. En el caso del spam, quizás el precedente más famoso sea el sentado a partir de *Compuserve Inc, v. Cyberpromotions*, en el cual *Compuserve* alegó que el envío masivo de correos electrónicos por parte de *Cyberpromotions* había producido daño físico al equipo del demandante y, además, había dañado su reputación y buenas relaciones con sus clientes.

5. La opción “opt out.”: las legislaciones que funcionan con esquemas de opt-out permiten el envío de correos masivos no solicitados a menos que el receptor le haya informado al spammer que no desea seguir recibiendo correos (opt-out específico) o bien el receptor se haya incluido en una lista o registro (registros de opt-out) a través de la cual se informa a los spammers que esa persona no desea recibir publicidad. Aunque el opt-out es una de las opciones preferidas al momento de legislar sobre spam presenta en sus dos versiones bastantes problemas. En el caso del opt-out específico, existe alguna evidencia que un número relevante de spammers utiliza las cláusulas de remoción para verificar la dirección de correo electrónico del receptor y no lo remueve de sus registros aún cuando este ha utilizado la cláusula de remoción según las instrucciones del spammer. Como resulta evidente, el problema de esta solución es que aún las comunicaciones que cumplan con estos requisitos podrían representar una cantidad suficiente para producir problemas a los proveedores de servicios de internet (quienes deberían invertir en software de filtro y bloqueo) y los usuarios (un ejemplo de esto es el servicio de bloqueo de Hotmail, el cual envía los correos comerciales hacia una carpeta de correo no deseado). El problema de esta solución, sin embargo, es que dicha carpeta utiliza parte del espacio disponible de cada usuario y, en el largo plazo puede saturar la capacidad de nuestro buzón de correo electrónico.

A lo anterior, no debemos olvidar el principal problema de la legislación en el caso de internet es la ausencia de fronteras físicas definidas. En el mundo que conocemos las fronteras demarcan las áreas donde un determinado Estado es soberano de imponer y hacer cumplir su legislación.

Una defensa frente a la “aterritorialidad” de internet consiste en sostener que esta puede ser corregida a través de tratados internacionales. Esto, sin embargo, supone uniformidad entre las diversas legislaciones sobre spam que, como se ha advertido, a la fecha no existe.



Junto al problema de la aterritorialidad de internet, aún es posible registrar tres inconvenientes más al momento de utilizar la legislación para regular el envío masivo de correos no solicitados. El primero es el dinamismo de la tecnología, el segundo es la legitimación de ciertas formas de correo no deseado al prohibir otras. Y finalmente, el tercero, tiene que ver con la especial protección que suele recibir la libertad de expresión.

El ciberespacio no tiene fronteras basadas en el territorio ya que el costo y velocidad de envío de la transmisión de un mensaje en la Red es casi completamente independiente de la ubicación física: los mensajes pueden ser transmitidos desde cualquier ubicación a cualquier ubicación sin arruinarse, degradarse o demorarse sustancialmente más y sin que ninguna barrera física o que pueda mantener lugares y personas remotamente alejados separados unos de otros.

Con lo anterior, puedo aventurarme a plantear de manera simple, como podría integrarse un Proyecto Ley anti spam en nuestro país, así:

Proyecto General de Ley Anti Spam para Guatemala

Exposición de Motivos

En este apartado podría resumirse lo que es el spam, los tipos de spam y el daño que actualmente causa en la economía de un país; lo cual ya se desarrollo en el presente trabajo.

Disposiciones Generales

Artículo 1. La presente ley será de carácter público y tendrá por objeto regular los correos electrónicos no deseados o no solicitados, conocidos como spam, debido a que en la actualidad es una actividad perjudicial dentro de la internet.

Artículo 2. El Estado será el tutelar de los derechos esenciales de privacidad e intimidad de los usuarios guatemaltecos que utilicen para comunicarse el correo electrónico; garantizando el debido uso y aprovechamiento de las direcciones de correos electrónicos, a efecto de proteger la seguridad y soberanía nacional, la seguridad, tranquilidad y confidencialidad de los usuarios del correo electrónico dentro de los sistemas y equipos de informática del Estado y de los particulares.

Artículo 3. Para efectos de la aplicación de la presente ley, deberá tenerse los siguientes conceptos:

- Mensaje de correo electrónico: será todo mensaje enviado a una dirección de correo electrónico.
- Dirección de correo electrónico: se referirá al destino de un mensaje expresado en una cadena de caracteres alfanuméricos, o nombre del usuario y seguido del nombre del proveedor del servicio de correo electrónico registrado en internet
- Receptor: toda persona que teniendo una cuenta de correo electrónico recibe un mensaje dentro de su cuenta.
- Remitente: será toda persona que teniendo acceso a una conexión de internet envía un mensaje electrónico a un receptor.
- Correo electrónico tipo spam: todo mensaje no solicitado o no deseado que se reciba por parte del receptor, distribuido a una lista masiva de direcciones de correo electrónico, cuyo contenido sea básicamente de: publicidad de productos o servicios; contenido político y religioso; juegos o apuestas; de contenido pornográfico, comercio sexual, información falsa, sistemas piramidales o cadenas. Así también se tendrá por spam a todos los correos electrónicos, no importando cual sea el mensaje enviados por cualquier persona que se haga pasar por otro remitente

Artículo 4. No deberá considerarse como spam, aquellos correos electrónicos cuyo contenido sea publicidad de productos y servicios, de carácter comercial, político, religioso, pornografía, juegos de asar, sistemas piramidales o cadenas, o de cualquier contenido similar que sea solicitado expresamente por el receptor al emisor. Sin

embargo, el receptor podrá en cualquier momento ser removido de las bases de datos del emisor y así revocar su consentimiento para ya no recibir más correos electrónicos. Luego la revocación del consentimiento, los mensajes que ingresen serán tomados como correos electrónicos no deseados o no solicitados, es decir, se les considerará como spam.

Artículo 5. Responsabilidad. Serán responsables de las infracciones o delitos relacionados al envío de correo electrónico no deseado o no solicitado, spam, los que:

- a. Toda persona individual o jurídica que envíe correos electrónicos no solicitados conteniendo publicidad comercial.
- b. Las empresas o personas beneficiarias de manera directa con la publicidad difundida.
- c. Los intermediarios de correos electrónicos no solicitados, tales como los proveedores de servicios de correos electrónicos.

Artículo 6. Autoridad competente. Le corresponderá al Ministerio de Economía, a través de la sección de Protección al Consumidor, la aplicación de la presente ley, a través de una Comisión Especializada en los correos electrónicos, tipo spam. Al momento de entrar en funcionamiento la Procuraduría del Consumidor, esta será la encargada, de la recepción de las denuncias respectivas, quien en su debida oportunidad las trasladará al Ministerio Público, para el ejercicio de la acción pública para la investigación de los delitos en que se incurra. (En este sentido deberá ampliarse y agregarse los delitos relacionados al spam, en nuestro ordenamiento penal, incluyéndose las penas respectivas.)

Artículo 7. Atribuciones de la Comisión especializada en correo electrónico tipo spam. La comisión se integrará y funcionará según los términos que autorice la autoridad superior competente, en el reglamento respectivo. Dentro de las atribuciones generales estarán:

- a. Llevar un registro de todos los remitentes, los cuales sean reportados por

los receptores, o bien descubiertos por los mecanismos automatizados que puedan existir.

- b. Llevar un registro de control, de todos los remitentes que se dedican a enviar correos electrónicos no deseados o no solicitados, a los receptores nacionales.
- c. Promover a nivel nacional una cultura y participación de los usuarios de internet que tienda a prevenir y repudiar la mala practica del envío de correos electrónicos no deseados o no solicitados, así como fomentar la participación de los usuarios del correo electrónico a que reporten estos de correos tipo spam a la comisión.
- d. Utilizar en la medida de las posibilidades del Estado, todos los medios informatizados para la detección de las posibles fuentes de envío de correos electrónicos tipo spam.
- e. Coordinar los avances internacionales relacionados al tema del spam y coadyuvar para la integración respectiva en la normativa del país.
- f. Recibir las denuncias relacionadas a los correos electrónicos tipo spam, las de los receptores que inclusive no obstante haber dado en un principio su autorización expresa, posterior hayan revocado la misma. Posterior de un análisis de las denuncias remitirlas con dictamen al respecto, al Ministerio Público para que inicie la investigación penal que corresponda.
- g. Ser el órgano técnico y consultor en materia de spam, o correos electrónicos no deseados o no solicitados.

Artículo 8. Prohibiciones. Queda prohibido:

- a. utilizar una computadora protegida, para enviar o transmitir múltiples mensajes de correo electrónico tipo spam, es decir, correos no deseados o no solicitados.
- b. Acceder por cualquier medio o servicio de internet para enviar mensajes que engañen o mal informen a los ciudadanos.

- c. Alterar materialmente la información en los títulos de los correos electrónicos de carácter comercial e intencionalmente distribuir los mismos como spam.
- d. Usar información que materialmente falsifique la identidad de una persona y que la misma sea utilizada para: registrar varias cuentas o direcciones de correos electrónicos; hacerse pasar por un proveedor de servicios de internet; crear y comercializar grupos o listas de direcciones de correos electrónicos.
- e. Hacerse representar como cualquier proveedor de internet y que con dicho nombre, se distribuyan correos no deseados o no solicitados, spam.
- f. Obtener direcciones de correos electrónicos de los usuarios de la red, utilizando cualquier medio informatizado o software de cualquier conexión de internet, que se encuentre dentro del territorio nacional, con el propósito de enviar correos electrónicos tipo spam. Así también será prohibido, la creación o comercialización de software o programas especializados para la captura ilegal de dirección de correos electrónicos, y que a la vez permita o facilite el envío de correos tipo spam.
- g. La transmisión y redistribución de todo correo electrónico no deseado o no solicitado expresamente, de contenido sexual que: anuncie explícitamente o disimule dicho contenido en el título (subject) del correo electrónico; al momento de abrir o desplegar el mensaje sea de contenido sexual; o que al abrir o desplegar dicho mensaje, contenga instrucciones para ingresar y obtener acceso a material de carácter sexual.

Artículo 9. Sanciones. Al momento de recibir una denuncia, la comisión con la autoridad competente, se determinará si constituye delito penal, para lo cual se remitirá lo actuado, y será en el ordenamiento penal que deberá agregarse los artículos necesarios para la sanción contra los delitos del spam. Dichas sanciones deberán ser de tipo pecuniario y de privación de libertad inclusive. Adicionalmente, la Comisión especializada en los correos electrónicos, tipo spam, podrá sancionar de manera

pecuniaria y amonestaciones publicas en los diarios de mayor circulación, a los emisores de dichos correos electrónicos.

Como vemos, la experiencia internacional demuestra que efectivamente una regulación anti spam no termina por completo el problema, como lo sería por ejemplo una regulación penal que no elimina la violencia, pero la regulación anti spam si contribuye a disuadir dicha mala practica; y actualmente la Comunidad Europea recomiendan se formulen leyes de esta índole para ser tomados en cuenta los demás países al momento de negociar con ellos, ya que quieren evitar “paraísos” para los delincuentes tipo spammers, y así garantizar a sus miembros el derecho a la privacidad e intimidad en la red.

En Guatemala, que ya se utiliza gracias a los medios informatizados, la firma electrónica y el comercio electrónico, es necesario que se tenga una legislación específica y orientada a dar seguridad informática, la cual vendría a ya no ver este problema como un simple inconveniente sino que sería bien enfocado en la preocupación del Estado guatemalteco, por garantizar efectivamente las relaciones de los ciudadanos en la internet.

4.2. Criterios para calificar el correo comercial no solicitado

Según lo señalado en el presente trabajo, podemos decir, que estaremos frente a un correo electrónico comercial no solicitado cuando no existe relación previa entre las partes y el receptor no ha consentido explícitamente en recibir la comunicación. Puede significar también que el receptor previamente ha buscado terminar una relación existente, usualmente instruyendo a la otra parte de no enviarle más comunicaciones en el futuro. Por supuesto no basta que se trate de correo no solicitado en los términos recién expuestos. Lo que, en principio, y lo califica como correo electrónico no solicitado como spam es su carácter comercial, la cantidad enviada o, desde luego, una mezcla de ambos.

Aún cuando la definición de comercial varía en las distintas legislaciones del mundo, que suele considerarse en el caso de las comunicaciones comerciales es la promoción de algún tipo de bienes o servicios, que no hayamos requerido.

4.3. Criterios para calificar el correo ilegal no solicitado

Tendremos un spam ilegal, cuando se utilicen recursos ajenos, ya que para su distribución el spam, aprovecha de Estafetas ajenas mal configuradas openrelay¹⁰.

Existe entre los spammers bases de datos de máquinas (IP) mal configuradas para poder ser usadas. El spam ilegal es uno de los más extendidos y suele ser el que viene en idioma inglés.

Entonces un correo electrónico no solicitado o no deseado, spam, será considerado ilegal cuando:

1. No cumpla con señalar la palabra “publicidad” o “publicidad para adultos”, según corresponda, en el campo del “asunto” (o subject) del mensaje.
2. No contenga el nombre o denominación social, domicilio completo y dirección de correo electrónico de quien emite el mensaje.
3. No incluya una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos, o de otros mecanismos basados en internet que permitan al receptor manifestar su voluntad de no recibir mensajes adicionales.
4. Contenga nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que transmite el mensaje.
5. Se envíe o transmita a un receptor que haya formulado el pedido para que no se envíe dicha publicidad.

¹⁰ Estafeta open-relay: son servidores de correo mal configurados que permiten encaminar correo desde cualquier dirección IP. Esto permite un uso indebido de recursos de la empresa por parte de personas ajena a la misma. Estas Estafetas son las preferidas por los spammers para inyectar mensajes de spam y destinado a miles o millones de destinatarios.

6. Contenga información falsa o engañosa en el campo del "asunto" (o subject), que no coincida con el contenido del mensaje; y también cuando el contenido del mensaje no fuera veraz.

Además, en todos los casos un correo electrónico calificará como ilegal si no cumple con las disposiciones y formalidades en defensa de la protección al consumidor y sobre publicidad comercial en defensa del consumidor.

4.4. Derechos y obligaciones del usuario y proveedor de servicios de internet

Los usuarios de correo electrónico a través del internet tienen los siguientes derechos, según las legislaciones más actualizadas, serán:

- a) Rechazar o no la recepción de correos electrónicos comerciales.
- b) Revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión del servicio de correo electrónico.
- c) Que su proveedor de servicio de correo electrónico cuente con sistemas o programas que filtren los correos electrónicos no solicitados.
- d) El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.
- e) Toda persona tiene derecho a que sean rectificadas, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.

Y dentro de las obligaciones de los proveedores, se menciona:

- a) Los proveedores de servicio de correo electrónico domiciliados dentro de un país específico, estarán obligados a contar con sistemas o programas de bloqueo y/o filtro para la recepción o la transmisión que se efectúe a través de su servidor, de los correos electrónicos no solicitados por el usuario.





CONCLUSIONES

1. Entre las más frecuentes violaciones de los derechos humanos en el tiempo actual, están las actuaciones de entidades particulares o públicas que recopilan información confidencial o personal de los individuos, sin que el dato sea verificado, ni conocido por la persona afectada; o ilegalmente manipulada, que generalmente es con fines de lucro.
2. El spam es un problema considerable y creciente para los usuarios, las redes e internet en general. Según datos de la Agencia Española de Protección de Datos -AEPD- el spam representa en la actualidad alrededor del 70 % del tráfico mundial de correo electrónico.
3. La libertad informática o autodeterminación informativa, ha sido denominada por el derecho comparado, como un nuevo derecho fundamental que tiene por objeto garantizar la facultad de las personas, para conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos y controlar su calidad; lo que implica la posibilidad de corregir o cancelar datos indebidamente procesados y disponer su transmisión.
4. Si los mensajes "spam" se han desarrollado a un ritmo tan espectacular, es porque alimentan una industria floreciente, pues ya existe un sistema bien organizado para escribir y poner en circulación virus y troyanos, que recopilan y venden luego la lista de máquinas infectadas por esos virus, con la información personal que en éstas se encuentran.



5. El derecho a la intimidad y a la privacidad se encuentran actualmente amenazados por la capacidad que posee, tanto el sector público como el privado, de acumular gran cantidad de información acerca de los individuos en forma digital, ya que se permite a tales entidades manipular, alterar e intercambiar datos personales a gran velocidad y bajo costo.



RECOMENDACIONES

1. El Organismo Legislativo guatemalteco debe reconocer que el fomento de un clima de confianza que garantice la seguridad y la protección de los datos personales, es un requisito previo e indispensable para que se desarrolle la sociedad de la información de forma efectiva, muy en particular el envío masivo de mensajes electrónicos no solicitados.
2. El Congreso de la República de Guatemala debe analizar la necesidad de una legislación en el ordenamiento jurídico guatemalteco, que permita garantizar efectivamente la seguridad de los datos personales; en especial, la dirección de correo electrónico, utilizado por personas individuales o jurídicas; y no sólo normar este problema en un solo artículo, como quedó en el Decreto Número 47-2008 del Congreso de la República Ley para el reconocimiento de las comunicaciones y firmas electrónicas.
3. El Congreso de la República de Guatemala debe tomar conciencia de lo mucho que beneficiaría al país, una legislación anti spam completa, ya que lo colocaría entre los vanguardistas y sería tomado muy en cuenta a la hora de que Guatemala participe en este mundo globalizado, en los tratados de libre comercio, que actualmente entre sus requisitos solicitan legislaciones que efectivamente brinden seguridad jurídica a las personas colectivas e individuales, en cuanto a la protección de la intimidad y privacidad de sus datos personales, incluido el atributo de la dirección del correo electrónico.
4. La Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala debe fomentar la actualización de temas como la ausencia de legislación contra el envío de correos electrónicos no solicitados o no deseados, a efecto de que se conozca, tanto por profesionales del derecho, por estudiantes; los cambios en la ciencia del derecho que han surgido con los avances informáticos en la actualidad.



5. El Congreso de la República de Guatemala, para lograr una verdadera protección de carácter constitucional a los derechos de intimidad y privacidad, debe preocuparse por legislar, con una norma específica que regule y controle lo relacionado al envío de correos electrónicos no solicitados o no deseados, llamados spam; que son enviados sin previa autorización a los usuarios guatemaltecos de correos electrónicos.



BIBLIOGRAFÍA

Agencia Española de Protección de Datos. **Guía para la lucha contra el spam.** 2005.

ALTMARK, Daniel Ricardo. **Informática y derecho.** Buenos Aires, Argentina. 1987.

CALVO, Alfonso Luis y CARRASCOSA GONZALEZ, Javier. **Conflictos de leyes y conflictos de jurisdicción en internet.** Madrid. 2001.

CARRION, Hugo Daniel. **Presupuestos para la punibilidad del hacking.** Tesis de grado, Facultad de Ciencias Jurídicas y Sociales, Universidad San Carlos. Guatemala. Julio 2001.

CORTE DE CONSTITUCIONALIDAD DE GUATEMALA. **Constitución Política de la República de Guatemala, y su interpretación por la Corte de Constitucionalidad.** Talleres Gráficos Serviprensa. Guatemala, 2004.

Diccionario enciclopédico Uthea. Barcelona, España. Ed. Hispano Americana Litografía Pegaso, Sociedad Anónima. 2000.

Diccionario jurídico Espasa. Espasa Siglo XXI. Edi.1998.

Diccionario pequeño Larousse. Editorial Larousse. Buenos Aires, Argentina, 1999.

JAVALOIS CRUZ, Andy Guillermo. **Delito informático.** Instituto de Investigaciones Jurídicas. Universidad Rafael Landívar. Guatemala, abril 2005.

KELSEN, Hans. **Derecho y paz en las relaciones internacionales.** Editorial Fondo de Cultura Económica. México, 1996.

MOLINER, María. **Diccionario de María Moliner** Edición digital. Copyright© 1996 Novel Inc.; Copyright © 1996.



MONTESINOS GUTIÉRREZ, Antonio. **La sociedad de la información e internet.** Madrid. 1999.

LIMA de la LUZ, María. **Delitos electrónicos.** Ediciones Porrúa. México. Enero-Julio 1984.

OSSORIO, Manuel. **Diccionario de las ciencias jurídicas políticas y sociales.** Editorial Heliasta. Buenos Aires, Argentina. 1981.

PALAZZI, Pablo. **El derecho y la alta tecnología.** Tomo II – Doctrina. Buenos Aires, Argentina. 1999.

TÉLLEZ VALDÉS, Julio. **Derecho informático.** Editorial Mcgraw-Hill Interamericana, S.A. México, 1995.

Legislación:

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, 1986.

Convenio para la protección de las personas en relación con el tratamiento automatizado de datos de carácter personal. Estrasburgo, 28 enero 1981.

Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal. Promulgada en España el 29 de octubre 1992

Ley de Privacidad. Promulgada en Estados Unidos el 31 de diciembre de 1974

Ley Número 34-2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico. Promulgada en España el 11 de junio de 2002