



**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

---

---



**FACULTAD DE DERECHO.  
SEMINARIO DE DERECHO PENAL.**

**“PROPUESTA DE CREACIÓN DE LEY ANTI-SPAM  
EN MATERIA PENAL.”**

TESIS PROFESIONAL  
PARA OBTENER EL TÍTULO  
DE LICENCIADO EN DERECHO.

PRESENTA:  
**ERIC ERNESTO RODRÍGUEZ GARCÍA.**

ASESOR DE TESIS:  
MTRA. LORENA PICHARDO FLORES.

CIUDAD UNIVERSITARIA

2013.



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



FACULTAD DE DERECHO  
SEMINARIO DE DERECHO PENAL  
OFICIO INTERNO FDER/ SP/34/04/2013  
ASUNTO: APROBACIÓN DE TESIS

**DR. ISIDRO ÁVILA MARTÍNEZ**  
**DIRECTOR GENERAL DE LA ADMINISTRACIÓN**  
**ESCOLAR DE LA U.N.A.M.**  
**P R E S E N T E.**

El alumno **ERIC ERNESTO RODRÍGUEZ GARCÍA**, con no. de cuenta: 301129400, ha elaborado en este Seminario a mi cargo y bajo la dirección de la LIC. LORENA PICHARDO FLORES, la tesis profesional titulada "PROPUESTA DE CREACIÓN DE LEY ANTI-SPAM EN MATERIA PENAL" que presentará como trabajo recepcional para obtener el título de Licenciado en Derecho.

La profesora, LIC. LORENA PICHARDO FLORES, en su calidad de asesor, informa que el trabajo ha sido concluido satisfactoriamente, que reúne los requisitos reglamentarios y académicos, y que lo aprueba para su presentación en examen profesional.

Por lo anterior, comunico a usted que la tesis "PROPUESTA DE CREACIÓN DE LEY ANTI-SPAM EN MATERIA PENAL" puede imprimirse para ser sometida a la consideración del H. Jurado que ha de examinar al alumno **ERIC ERNESTO RODRÍGUEZ GARCÍA**.

En la sesión del día 3 de febrero de 1998, el Consejo de Directores de Seminario acordó incluir en el oficio de aprobación la siguiente leyenda:

"El interesado deberá iniciar el trámite para su titulación dentro de los seis meses siguientes (contados de día a día) a aquél en que le sea entregado el presente oficio, en el entendido de que transcurrido dicho lapso sin haberlo hecho, caducará la autorización que ahora se le concede para someter su tesis a examen profesional, misma autorización que no podrá otorgarse nuevamente sino en el caso de que el trabajo recepcional conserve su actualidad y siempre que la oportuna iniciación del trámite para la celebración del examen haya sido impedida por circunstancia grave, todo lo cual calificará la Secretaría General de la Facultad"

Sin otro particular, agradezco anticipadamente la atención que le dé a la presente solicitud, y aprovecho para enviarle un saludo cordial.

**ATENTAMENTE**  
**"POR MI RAZA HABLARÁ EL ESPÍRITU"**  
Cd. Universitaria, D. F., 10 de Abril de 2013.

**MTRO. CARLOS ERNESTO BARRAGÁN Y SALVATIERRA**  
**DIRECTOR DEL SEMINARIO**



CEBS/cch

**100** UNAM  
CENTRO DE INVESTIGACIONES Y  
ESTUDIOS SOCIALES

## **AGRADECIMIENTOS.**

*Principalmente a Dios, por darme fuerzas y permitirme llegar a este momento tan importante en mi vida y aún más el conducirme en mi instrucción académica.*

*A mis padres, por ser grandes pilares en mi vida e inculcarme hábitos, valores, principios, pero sobretodo el gran apoyo que me han brindado a cada instante, sus esfuerzos para salir avante en mi formación profesional, se ven reflejados en el subsecuente ensayo.*

*A mi hermana, mi sobrina y mi familia en general, por darme su confianza y alentarme, para hacer realidad mis sueños.*

*A mis Abuelos, peculiarmente los que están en el cielo, sus enseñanzas las tendré presentes, ya que fueron testigos del difícil camino que me tomo llegar a esta fantástica carrera y cumplir una de mis grandes metas.*

*A ti, por respaldarme a salir adelante en los momentos difíciles y aún más en los felices, por ser una parte esencial en mi carrera y en mi vida e inspirarme a culminar mis propósitos.*

*A mi alma mater la Universidad Nacional Autónoma de México, en especial a la Facultad de Derecho, por permitirme formar parte de ella y brindarme las bases necesarias como profesionalista.*

*Al Seminario de Derecho Penal, particularmente al Mtro. Carlos Ernesto Barragán y Salvatierra, que en todo momento me brindaron confianza, un trato cordial en los trámites y elaboración de mi proyecto.*

*A la Mtra. Lorena Pichardo Flores, que siempre le estaré agradecido por la paciencia, apoyo y conocimientos que me brindo para completar y estructurar la presente investigación.*

**PROPUESTA DE CREACIÓN DE LEY ANTI-SPAM  
EN MATERIA PENAL.**

**ÍNDICE.**

<b>INTRODUCCIÓN.</b>	<b>I</b>
----------------------	----------

**CAPÍTULO I: MARCO HISTÓRICO.**

**ORÍGEN DEL CORREO ELECTRÓNICO COMERCIAL NO SOLICITADO: SPAM.**

1.1 Historia de la computación, Internet y Correo Electrónico.	1
1.1.1 Historia de la computación.	1
1.1.2 Historia del Internet.	6
1.1.3 Historia del correo electrónico.	9
1.2 Antecedentes e historia del término SPAM.	12
1.3 Convenciones Internacionales sobre el Spam.	14

**CAPÍTULO II**

**MARCO JURÍDICO.**

2.1 Legislaciones ANTI-SPAM más importantes del mundo.	19
2.2 Problemática legal en México.	42
2.2.1 Constitución Política de los Estados Unidos Mexicanos.	42
2.2.2 Código Penal Federal.	48
2.2.3 Ley de Datos Personales en Posesión de los Particulares.	48
2.2.4 La Ley Federal de Protección al Consumidor.	49

### **CAPÍTULO III**

#### **MARCO CONCEPTUAL.**

3.1 Campo de estudio del Derecho Informático.	53
3.2 Definición del SPAM.	58
3.3 Sujeto activo del Spam.	61
3.4 Características del Spam.	64
3.5 Medios Informáticos donde se presenta el Spam.	65
3.6 Temas del Spam.	68
3.7 Definiciones a fines.	70
3.8 Daños que ocasiona el Spam.	75
3.9 Tipos de Spam más comunes en México.	78

### **CAPÍTULO IV**

#### **ANÁLISIS DOGMÁTICO DEL SPAM.**

4.1 Conducta.	83
4.2 Tipicidad.	90
4.2.1 Elementos objetivos del tipo penal.	92
4.2.2 Elementos normativos del tipo penal.	96
4.2.3 Elementos subjetivos del tipo penal.	99
4.3 Antijuridicidad.	102
4.4 Imputabilidad.	108
4.5 Culpabilidad.	111
4.6 Punibilidad.	115
4.7 Fases de ideación del delito y consumación.	117
4.8 Concurso de personas y de delitos.	118

**CAPÍTULO V**  
**EL PROBLEMA DE LA AUSENCIA DE UN TIPO PENAL EN EL**  
**CÓDIGO PENAL FEDERAL QUE SANCIONE EL SPAM.**

5.1 Fortalezas y debilidades de la regulación en la Ley Federal de Protección al Consumidor.	124
5.2 Importancia de realizar una Ley Anti-Spam.	127
5.3 Tipos de Spam más recurrentes en México	130
5.3.1 Consideraciones que debe tomar el legislador para prevenir, proteger y sancionar el Spam.	140
<b>CONCLUSIONES.</b>	145
<b>PROPUESTA.</b>	148
<b>BIBLIOGRAFÍA.</b>	155

## INTRODUCCIÓN.

Desde los inicios del hombre prehistórico ante la necesidad de establecer relaciones con sus semejantes, se ve forzado a utilizar cualquier instinto o medio para comunicarse, abarcando desde señales de humo, invención de lenguajes plasmados en papel, por la necesidad de establecer comunicación a distancia, dando paso a instrumentos o medios tales como, el telégrafo, el periódico, el teléfono, la radio, la televisión, mismos que hasta ahora se siguen utilizando en nuestra cultura.

Dichos medios han dado paso a la invención de la creación de la computadora, e Internet los cuales son lo más modernos y eficaces que tenemos en nuestra época, pero el proceso para tener las computadoras o equipos con los que contamos no fue una tarea fácil, ya que tuvieron que pasar varios años e intentos de creación desde la primera computadora la cual abarcaba una habitación en su totalidad, es decir, era enorme, pero era capaz de resolver operaciones, dando lugar a las diferentes “generaciones de las computadoras”, hasta llegar a la nuestra denominada “era digital” en la cual estamos inmersos de tecnología, a través de medios electrónicos de comunicación, como lo son microcomputadoras, etc.

Aquí es donde el correo electrónico vino a revolucionar en tiempo y forma, lo concerniente a la comunicación a distancia, ya que por este medio podemos transmitir mensajes, y llegar a establecer relaciones desde cualquier parte del mundo, es decir, podemos enviar y recibir información escrita e imágenes, lo único que necesitamos es una dirección de correo electrónica. La cual podemos obtener en cualquier servidor que cubra dicha plataforma.

Dicha herramienta es utilizada en un gran porcentaje de los usuarios en Internet, por su prontitud y el bajo costo que representa utilizarlos. La ventaja de este medio es la facultad de almacenamiento en Internet, es decir, podemos

guardar aquella información que nos resulte importante y acceder a ella en el momento que deseemos. Y es importante señalar que no es necesario que el emisor y receptor se encuentren conectados, ya que estos tienen la facultad de llegar directamente a la bandeja de entrada de nuestro correo electrónico.

Lamentablemente en esta magnífica herramienta de medio de comunicación, surge una modalidad muy perjudicial denominada Spam, el denominado correo electrónico comercial no solicitado.

El problema que se presenta con el Spam es que se envía a miles de direcciones electrónicas, este puede llegar a saturar nuestras bandejas de entrada e incluso llega a causar un tráfico de información en Internet, llegando a disminuir la rapidez de la banda ancha.

El correo electrónico comercial no solicitado posee contenido e información fraudulenta o aparentemente auténtica, cuya característica induce a caer en el error. Alguien puede estar completamente seguro de este aspecto, brindaremos información confidencial, y en consecuencia llegar a robar nuestra identidad, aspecto muy importante, mismo que veremos en la presente investigación.

Un aspecto del Spam es que los sujetos activos son individuos expertos en sistemas computacionales, su actividad consiste en la creación, redacción y envío de mensajes, los cuales pueden infectar computadoras con virus realmente poderosos, llegando a modificar, dañar o perder información valiosa.

Actualmente, el Spam no sólo se presenta en el correo electrónico, sino que se está expandiendo en la telefonía móvil, en su mayoría en teléfonos inteligentes y en las denominadas redes sociales.

En nuestro país no existe una legislación que regule el correo electrónico comercial no solicitado y por lo tanto es necesario, que exista una disposición

penal que especifique una definición del SPAM, sus modalidades, medios comisivos, los sujetos tanto activo y pasivo, así como la autoridad competente para perseguir e investigar el ilícito.

Varios países tienen legislaciones vigentes para combatir las diferentes acciones del mismo, logrando reducir el impacto que produce en la red, pero es de vital importancia contar con una legislación propia, sin la necesidad de recurrir a convenios o a que el Juez recurra a la interpretación, o desconocimiento de la norma.

Esta tesis, trata de hacer conciencia en la implementación de medidas de prevención, leyes adecuadas, una cultura que fomente el uso adecuado del correo electrónico y por consiguiente de Internet, así como también foros, exposiciones y convenciones tanto nacionales como internacionales, que den solución adecuada ante los ataques que sufren los usuarios, sin la radical medida de eliminar por completo al correo electrónico.

A continuación se aborda la escasa mención en la legislación existente en nuestro país, al correo electrónico comercial no solicitado visto desde el área comercial y publicitaria.

**CAPÍTULO I: MARCO HISTÓRICO.**  
**ORIGEN DEL CORREO ELECTRÓNICO COMERCIAL**  
**NO SOLICITADO: SPAM.**

**1.1 Historia de la computación, Internet y correo electrónico.**

**1.1.1 Historia de la computación.**

La creación de las computadoras no fue un hecho espontáneo, este surgió ante la necesidad de resolver problemas, que para el hombre le costarían mayor tiempo en resolverlos. Aunque no fue tarea fácil, ya que se tenían que realizar bastantes trabajos para poder abarcar dichas necesidades.

Su origen se remonta al siglo XIX, cuando el hombre requirió hacer mayores cálculos que abarcaban la solución de problemas comerciales, y elaboro el ábaco, primer antecesor de la computadora.

El **Ábaco** es una herramienta que sirve para poder realizar diversas operaciones matemáticas, su forma es rectangular, este mismo que está compuesto por bolitas de colores, insertadas en alambres y cada una tiene un valor determinado. Se dice que surgió hace alrededor de 5000 años y actualmente se sigue utilizando.

La primera máquina sumadora fue la **Pascalina**, denominada así por su creador Blaise Pascal filósofo y científico. Poco tiempo después Charles Babbage ideó la máquina de diferencias para realizar los cálculos automáticos.

El gran invento que dio paso a las computadoras fue la tarjeta perforada para el procesamiento de datos. Fue Herman Holerith quien tomó como base los telares para hacer decoraciones, en la invención de estas tarjetas.

El evento importante dentro de la computación es la construcción de la computadora electrónica, el cual sucedió en el año de 1947 en la Universidad de Pensilvania, con la colaboración de los ingenieros John Mauchly y John Eckert y fue la denominada, ENIAC (*Electronic Numerical Integrator And Calculator: Computadora e Integrador Numérico Electrónico*), aunque la computadora abarcaba todo un sótano de dicha universidad, este invento era capaz de realizar cinco mil operaciones aritméticas en un segundo, fue un gran logro, pero ese tamaño inmenso tenía que resolverse.

Es así como se integra a este gran equipo el ingeniero y matemático húngaro, ante la necesidad de que ese inmenso volumen de maquinaria se redujera John Von Neumann el encargado de liderar dicho proyecto, sus ideas causaron revolución en cuanto al desarrollo de las computadoras y por esto es considerado el padre de la computación. Este equipo creó la EDVAC (*Electronic Discrete Variable Automatic Computer: Computadora automática electrónica Variable discreta*), una característica esencial es que las instrucciones de un programa puedan estar almacenadas en la computadora. Este diseño se sigue utilizando en la creación de nuestras computadoras.

Para entrar en materia es necesario dar una definición clara y común de lo que conocemos hoy como computadora:

“Equipo informático de tratamiento automático de datos que contiene los órganos (o elementos) necesarios para su funcionamiento autónomo.”<sup>1</sup>

En su concepción más técnica:

“La computadora es un dispositivo electromecánico capaz de realizar todo tipo de cálculos y procesamientos de información como respuesta

---

<sup>1</sup> Téllez Valdés, Julio, *Derecho informático*, 4ª. ed., México, Mc Graw Hill, 2008, p. 439.

a una serie de comandos e instrucciones, que le permiten realizar las tareas de entrada, procesamiento, almacenamiento y salida.”<sup>2</sup>

Ahora bien daremos pauta, de manera breve a la evolución de las computadoras, la cual se dividió en las siguientes generaciones:

## 1) PRIMERA GENERACIÓN (1946-1958).

Se caracterizó por la utilización de tubos al vacío. Para acceder a la información se hacía en milisegundos, para almacenarla, se usaban las tarjetas perforadas como dispositivo de almacenamiento auxiliar. Se contribuyó en cuanto al aumento de la velocidad de cálculo de las computadoras; destaco “la ENIAC, ya que era capaz de resolver varias operaciones matemáticas en cuestión de segundos, otros ejemplos de este tipo de computadoras son: ASCC, (*Automatic Sequence Controlled Calculator: Calculadora controlada de secuencia automática*), más conocido como Harvard Mark I o Mark I, y UNIVAC, (*Universal Automatic Computer I: Computadora automática universal*).”<sup>3</sup>

- MARK I: Howark Aiken profesor de la Universidad de Harvard (en donde fue utilizada 10 años), junto con la IBM (*International Business Machines: Corporación Internacional del Negocio de Maquinas*), inventó esta nueva computadora que resolvía problemas matemáticos y aritméticos a los ingenieros, físicos y matemáticos.
- ENIAC: Fue creada en el año de 1946 por el Dr. John Mauchly y Eckert, la cual era más veloz que las anteriores computadoras.
- UNIVAC: Primera computadora desarrollada con fines comerciales. Creada por Mauchly y Eckert, se usó en la Oficina de Censo de los Estados Unidos.

---

<sup>2</sup> Chacón Alvarado, Lucía, *Automatización de la Biblioteca*, San José, Costa Rica, Universidad estatal a distancia, 2002, p.13.

<sup>3</sup> Navarro Islas, Jorge, *Aspectos legales de las tecnologías de información y de las comunicaciones y comercio electrónico*, México, AMIPCI, 2008, pp. 19-25.

## **2) SEGUNDA GENERACIÓN (1959-1964).**

Se caracterizaban por la utilización de transistores que sustituían los tubos al vacío. Entre las ventajas de estos transistores encontramos la de requerir menos poder, generar menos calor, y ser más baratos que los tubos al vacío. El acceso de tiempo era en microsegundos, se usó la cinta magnética como dispositivo de almacenamiento secundario y auxiliar.

Surgieron computadoras de un menor tamaño, más rápidas, a comparación de la anterior generación; se comienzan a producir programas de sistema y se utilizan estas máquinas para el procesamiento de datos. Tenían cierta compatibilidad entre computadoras de un mismo fabricante y se utilizaban lenguajes de programación de bajo nivel. Entre los ejemplares de computadoras de esta generación encontramos: la IBM 1410 catalogada como una computadora comercial de tamaño pequeño a mediano, la IBM 160, computadora científica, y la IBM 7094, computadora científica grande.

## **3) TERCERA GENERACIÓN (1964-1970).**

La utilización de circuitos integrados sustituyen los transistores. Se utilizaron técnicas de microelectrónica que permitían que sus transistores fueran más duraderos y pequeños. Destacan mucho estas computadoras, ya que se incrementa la velocidad de tiempo de operación que era medido en nanosegundos, permitía la posibilidad de comunicación de datos y confiabilidad en cuanto al resultado de las mismas; existe disminución en cuanto al costo y tamaño de los equipos.

Se da la integración de *hardware* (Dispositivos físicos), y *software* (Conjunto intangible de datos y programas), se podían procesar más de dos funciones al mismo tiempo.

Entre las computadoras de esta generación se encuentra la IBM 360 y su predecesora la IBM 370 que tenía una mayor potencia que la anterior.

#### **4) CUARTA GENERACIÓN (a inicios de 1971-1982).**

Son computadoras más pequeñas, con una comunicación de datos más eficiente y lenguaje de programación más poderoso. Tiene multiprogramación y multiproceso, un software más avanzado y dispositivos de entrada y salida más efectivos.

Aparece el microprocesador y las redes de computadora; se utiliza el *disquete* para almacenar datos; entran al mercado microcomputadoras destacando la IBM. Se pueden colocar datos dentro de un *chip* (componentes electrónicos en miniatura, llamados semiconductores).

#### **5) QUINTA GENERACIÓN (1983-1989).**

Con todos los acontecimientos de las computadoras, se llegó a lo que actualmente conocemos como microcomputadoras, pero con la diferencia de que son más rápidas, con gran capacidad de cálculo y almacenamiento. Además existe una interconexión las mismas computadoras, dispositivos y redes, es decir, podemos utilizar simultáneamente varios microprocesadores. Desarrollo de grandes sistemas operativos y no podemos olvidarnos del Internet el cual es de mucha ayuda, pero hay que saber darle un uso adecuado.

#### **6) MODELO DE VON NEUMANN (1990-hasta la actualidad).**

Las computadoras digitales actuales se ajustan al modelo propuesto por el matemático John Von Neumann. De acuerdo con él, una característica

importante de este modelo es que tanto los datos como los programas, se almacenan en la memoria antes de ser utilizados.

Cada día la evolución fue aún mayor, las computadoras contaban con software y hardware innovadores que cubrían no sólo las necesidades básicas de las personas y de las empresas, ahora cuentan con áreas de entretenimiento, entre las que encontramos juegos, música, información de noticias, espectáculos etc.

Las computadoras actuales son capaces de resolver más de un millón de millones de operaciones aritméticas por segundo, a través del ancho de banda, se pueden transmitir datos a una mayor velocidad.

La idea de adquisición de nuevas tecnologías permitió que las herramientas de las computadoras también fueran impulsadas, tanto instituciones, empresas científicas y culturales se interesaron en nuevos proyectos, tales como el Internet, por ello daremos paso al análisis de los que es considerado la red más importante hablando científica, cultural y tecnológicamente alrededor del mundo.

### **1.1.2 Historia de Internet.**

Internet nace en los años 60's, sin embargo, los primeros indicios se remontan al año de 1957 en plena Guerra Fría entre los bloques militares de la URSS Y EEUU. Se creó una carrera espacial entre estas dos potencias como un aspecto de la Guerra Fría. Por su parte, la URSS, lanza su primer Satélite Sputnik, en un intento de superar este proyecto, Estados Unidos es quien, en su programa Júpiter del USARMY (ejército de los Estados Unidos) lanza satisfactoriamente, el Explorer 1, el 31 de enero de 1958. En este inter de tiempo, el gobierno de los Estados Unidos, al querer mantenerse a la cabeza en la carrera

militar crea una red informática<sup>4</sup> descentralizada denominada ARPANET (*Advanced Research Projects Agency Network*: Red de la Agencia de Proyectos de Investigación Avanzada), lo que sólo fue un proyecto de carácter militar y gubernativo, pronto lo adoptaron y se unieron conexiones de universidades, centros de investigación, empresas e instituciones que tuvieran la necesidades de un avance tecnológico, seguro o de mera investigación.

En realidad lo que ostentaba el ejército norteamericano era un sistema, el cual debería ser tan seguro que tendría que soportar cualquier ataque a sus computadoras y líneas, inclusive cuando alguno de ellos fuera destruido, con la opción de poder reponerse al ataque.

Ante esta demanda de necesidades ARPA (*Advanced Research Projects Agency*: Agencia de Proyectos de Investigación Avanzada), desarrollo un sistema, que tuviera la opción de varias rutas que alternaran la comunicación, utilizando los recursos disponibles, sin la limitación de contar con sólo una ruta.

En 1972 más de 50 Universidades trabajaban en proyectos militares, que se conectaban en ARPANET, esta situación causo que universidades y centros de investigación aumentarán la demanda para poder contar con este nuevo recurso informático, razón que impulso a que el Pentágono tomara la decisión de crear una segunda red denominada MILNET (*Military Network*: Red Militar), de uso exclusivo del ejército.

Fue hasta 1983 cuando una tercera red la CSNET (*Computer Science Network*: Red de Informática), (cuyo destino era simplemente científico) se conecta a ARPANET y a MILNET consagrando con esta triple conexión el

---

<sup>4</sup> La red informática es un conjunto de computadoras y periféricos, interconectados entre sí, que permiten que se transmita información y se comparta recursos. Para que una red pueda funcionar debe contar con el hardware necesario: tarjeta de red, router, swicht, cableado, concentradores, repetidores, etc. Una red puede estar montada alrededor de uno o más servidores, que son computadoras potentes en cuanto a microprocesador, memoria y capacidad de almacenamiento.

Las terminales son otras computadoras que se conectan al servidor y entre ellos. Los terminales pueden carecer de software propio y utilizar el del servidor, sirviendo como meros transmisores y receptores de datos, pero, generalmente, cuentan con su propio sistema operativo y otro software necesario dependiendo de las necesidades y requerimientos de la empresa.

nacimiento de Internet, esto se logró gracias a que compartía cierta característica, un mismo protocolo de comunicación (idioma). ARPANET no fue eterno ya que surgió la NSFNET (Red de la Fundación Nacional de Ciencias), la característica que aportó esta red, es que fue capaz de conectar varias redes de carácter académico, a más centros de investigación. Con esta aportación ARPANET se vió obligado a darse de baja en marzo de 1990 y CSNET dejó de existir en 1991, cediendo su lugar a INTERNET.<sup>5</sup>

Se ha venido explicando la historia del Internet, por lo que es relevante que se dé una definición de cómo se concibe:

“Internet es una libre asociación de miles de redes y millones de computadoras alrededor del mundo, que trabajan juntas compartiendo información. (Finnie Scott, Internet and on line services).”<sup>6</sup>

En una definición más técnica:

“Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP *Transmission Control Protocol* (TCP); *Internet Protocol* (IP), garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.”<sup>7</sup>

Esta inmensa red, tiene como aspecto a destacar que es descentralizada, autónoma, de carácter global y comparte un lenguaje común con el cual podemos interactuar.

---

<sup>5</sup> 1970 Vinton Cerf escribe por primera vez la palabra Internet. La escena tiene lugar a principios de los setenta en un hotel de San Francisco. Vinton, considerado el padre de la red, escribió la palabra Internet en el dorso de un sobre intentando explicar a sus compañeros la idea que había tenido sobre cómo distribuir información a través de la red que entonces se conocía como Internet. Este diseño sería la base del protocolo TCP/IP, que rige aún las comunicaciones por Internet.

<sup>6</sup> Pardini, Aníbal Alejandro, *Derecho de internet*, Buenos Aires, Argentina, la Rocca, 2003, p. 39.

<sup>7</sup> Disponible en: <http://es.wikipedia.org/wiki/Internet>, consultada el 5 febrero 2011 a las 12:30 horas.

La **www** (*World Wide Web*: Red Informática Mundial), fue desarrollada conjuntamente en 1989 por Timothy Berners-Lee y Robert Cailauu, para la Organización Europea para la Investigación Nuclear, más conocida como Centro Europeo de Física de Partículas (CERN), la idea principal era que los físicos de todo el mundo se comunicaran. Actualmente cualquier persona utiliza las siglas, como en el buscador principal. Internet en 1990 alcanza la cifra de 313 000 servidores, países como España, Argentina, Austria, Brasil, Chile, Irlanda, Suiza y Corea del Sur se pudieron conectar. Cabe señalar que México logro conectarse a Internet en 1989 siendo el primer país sudamericano en hacerlo.

### **1.1.3 Historia del correo electrónico.**

El Internet fue el mayor invento, en la historia de la computación, pero para que este gran avance existiera, primero se creó una herramienta especial que fue el correo electrónico, su nacimiento se dio antes del Internet.

En las primeras computadoras, había por lo general una máquina o procesador central que se comunicaba con diversos terminales, que en ese entonces era una pantalla y un teclado por lo general, y de los cuales los usuarios que accedían a ellas disponían a menudo de un buzón de correo que se usaba para la mensajería interna dentro el propio servidor, fue en 1961 en el Instituto Tecnológico de Massachusetts (MIT) donde se hizo la demostración de dicho sistema. Pronto su uso se extendió considerablemente y en 1966 se extendió para emplearse en redes de computadoras.

La aparición del símbolo (@) en las direcciones de correo electrónico se da en el año de 1971, cuando Ray Tomlinson eligió el arroba, para separar el usuario de la computadora en la que se arroja la casilla de correo. En inglés, la arroba se traduce como "At", en castellano "en". Por ejemplo `eric@hotmail.com`, esto significa Eric en Hotmail. En informática, se utiliza mayormente en las direcciones

de correo o mail. Separa el nombre de usuario y el nombre del proveedor de correo.<sup>8</sup>

Lo que ayudo a que el correo electrónico evolucionara y se convirtiera en lo que actualmente conocemos, fue la aparición de ARPANET, ya que su innovación era la de separar los mensajes que se comunicaban a través de la red, en paquetes de datos o datagramas, entre sus más grandes ventajas encontramos, que un mismo canal de comunicación podía usarse para comunicar muchas computadoras a la vez y la separación de paquetes, porque la información podía encaminarse por vías diferentes, esto ayudaba a que la comunicación fuera independiente y segura de estado de las líneas de transmisión de la información.

Para adentrarnos un poco en el tema, daré la definición sobre el correo electrónico. Según el diccionario de la Real Academia Española<sup>9</sup>:

“Sistema de comunicación personal por ordenador a través de redes informáticas.”

Para el Dr. Julio Téllez Valdés:

“Sistemas telemáticos de registro de transmisión de comunicación interpersonales que permiten, según sea el caso, enviar mensajes o acceder a ellos por medio de un dispositivo central; el envío de esos mensajes se da bajo el control del emisor y la recepción bajo el control del destinatario.”<sup>10</sup>

El correo electrónico permite a los usuarios enviar y recibir mensajes a través de la red, llegando a un buzón (servidor) donde permanecen hasta que el

---

<sup>8</sup> Diccionario de informática Alegsa. disponible en: <http://www.alegsa.com.ar>. Consultada el 07 de marzo 2011 a las 15:00 horas.

<sup>9</sup> Real Academia Española disponible en: <http://www.rae.es/RAE/Noticias.nsf/Home?ReadForm>. Consultada el 14 de marzo 2011 a las 13:00 horas.

<sup>10</sup> Téllez Valdés, Julio, op. cit., nota 1, p. 440.

usuario decida “abrirlos” o leerlos. Su funcionamiento básicamente es poder enviar mensajes entre computadoras personales o entre dos terminales de una computadora central, estos se archivan en un buzón. Cuando decidimos enviar un e-mail, se nos requerirán los siguientes datos:

- **Nombre del Destinatario:** puede ser a una o varias direcciones de correo electrónico.
- **Asunto:** Se plasma de forma breve un título que aparecerá en la bandeja de entrada del correo, para saber el motivo por el cual se envió.
- **Texto:** Varía según lo que se desea expresar, por el texto se puede entender no sólo lectura, sino videos, imágenes, etc.

De este sistema, se advierte la alusión al correo común, ya que se cuenta con un remitente, un destinatario (dirección de correo), asunto, el medio (que es el correo electrónico), y un buzón (bandeja de entrada).

A través de este medio podemos comunicarnos con cualquier persona, en cualquier parte del mundo y de manera instantánea; esto puede realizarse con una cuenta de correo electrónico, misma que puede adquirirse en cualquier empresa que ofrezca este servicio en el Internet.

Los elementos para comunicarnos por medio del correo electrónico son: contar con una dirección de correo electrónico, la cual sirve para poder identificarnos con todas aquellas personas con quienes deseamos enviar y recibir determinada información.

Para obtener una dirección de correo electrónico tenemos que proporcionar datos personales para adquirir dicho servicio, para esto tenemos que determinar, como queremos nombrarnos en este medio, ya que puede ser un nombre propio

y/o un sobrenombre; después seguirá el símbolo de la arroba (@), el cual todos conocemos en Internet y por último el nombre de la empresa o proveedor con la que obtuvimos sus servicios, ya sea de forma gratuita o de paga.

Considerando que el correo electrónico, es la manera más rápida y eficaz para comunicarnos en cualquier parte del mundo, grandes compañías que ofrecen este servicio como son Yahoo, Hotmail, y Google; mismas que compiten para incrementar el número de usuarios inscritos en dichas empresas.

Aparentemente el uso de este medio de comunicación suele ser seguro y confiable, veremos que lamentablemente esto no es así, ya que el gran problema que se presenta a los que cuentan con una o varias direcciones de correo en Internet, es al "SPAM" (el cual definiré en el tercer capítulo).

La mayoría de los usuarios, entran a sus cuentas de correo y abren la bandeja de entrada y si encuentran una carpeta que diga Spam, el mensaje lo borran o lo eliminan, esta acción no resuelve de fondo la problemática, porque al día siguiente vuelven a aparecer y en el peor de los casos habrá en mayor cantidad, las consecuencias serán graves si se abre y ve el mensaje, porque hay la posibilidad que se desarrolle un virus que afecte en parte el sistema central de nuestra computadora o en el peor de los casos afecta de forma total y permanente al sistema.

## **1.2 Antecedentes e historia del término SPAM.**

El origen de la palabra Spam es estadounidense. La palabra Spam designa a un alimento enlatado consistente en carne de cerdo picada con especias originalmente llamada *Hormel's Spiced Ham*. Posteriormente en 1937 "*Shoulder Pork and Ham/SPiced Ham*", dio su nombre de las letras SP de la palabra en

inglés *SPICE* (especias) y *AM*, de *HAM* (jamón).<sup>11</sup> Su gran éxito lo convirtió en una marca genérica, que tuvo tanto impacto que el mismo fabricante redujo su nombre, denominándolo sólo: SPAM. Este producto enlatado alimentó a los soldados soviéticos y británicos en la Segunda Guerra Mundial.

Algunas de las versiones a considerar sobre el SPAM son las siguientes:

- Toma el nombre de un sketch del grupo cómico inglés *Monty Python*, en el que la camarera de un restaurante describe los platillos del menú a una pareja, pero todos los platillos contienen Spam, sin opción para comer otra cosa.
- Existe otra versión de su origen el 3 de mayo de 1978, aproximadamente 393 empleados de ARPANET (el predecesor de Internet), recibían con sorpresa un correo de la compañía de computadoras DEC (*Digital Equipment Corporation*: Corporación de Equipos Digitales), invitándoles al lanzamiento de un nuevo producto.
- Una fecha en la cual por error surge el denominado Spam, sucedió en 1991 cuando un niño de 9 años se encontraba grave de salud, y recibía correos de todo el mundo para reanimarlo, motivo por el cual logro imponer un record mundial.

Sin embargo se considera que el acontecimiento, realmente importante con respecto al envío de correo electrónico no solicitado, surge el 5 de marzo de 1994, cuando una firma de abogados, **Canter And Siegel**, publica en USENET un mensaje de anuncio de su firma legal; el día después de su publicación, facturó cerca de 10 000 dólares por representar los casos de sus amigos y lectores de la red, desde esa fecha se obtuvo a nivel mundial el primer registro del correo no solicitado denominado “Spam”, aunado al avance de la tecnología, que desato que

---

<sup>11</sup> Guerrero Cañongo, Juan Antonio, *Los mejores Secretos para ganar Dinero en Internet*, México, Panorama Editorial, S. A. de C. V., 2007, p. 50.

este tipos de correos se emitieran de manera masiva alrededor del mundo; aunque con fines diferentes y no muy convenientes.

Además del correo electrónico otras tecnologías en Internet que han sido objeto de esta problemática, incluyen grupos de noticias USENET, motores de búsqueda, wikis, foros, blogs, a través de pop-up (ventana emergente) y algunas imágenes y textos de la web. Actualmente ha tenido como objetivo los teléfonos móviles, al mandar un mensaje de texto con publicidad y los sistemas de mensajería instantánea.

Si bien es cierto que sólo debemos recibir correos, de aquellas personas a las cuales les hemos proporcionado, nuestra dirección electrónica, que tenemos la certeza de quien se trata, o simplemente que es tema de nuestro interés. Realmente esto no sucede así, ya que diariamente se presenta este problema, me he permitido investigar y abordar la problemática, a modo que se pueda dotar a las personas u organizaciones del sector público, así como privado, de las formas adecuadas para detectar, prevenir y solucionar las consecuencias del SPAM a tiempo.

### **1.3 Convenciones Internacionales sobre el Spam.**

Ante la problemática de la aparición del Spam a nivel mundial, tanto los países como las organizaciones internacionales, se preocuparon por establecer medidas que combatieran al correo electrónico comercial no solicitado, existiendo la cooperación entre los gobiernos, fue posible llevar acabo la realización de Convenciones a nivel Internacional, donde expertos en materia informática, establecieron una serie de medidas acordes a la problemática a tratar, como se verá a continuación.

- **La Organización para la Cooperación y el Desarrollo Económico (OCDE).**<sup>12</sup>

En 2006, dio a conocer el *Anti-Spam Tool Kit* (Kit de herramientas de Anti-Spam), una iniciativa del grupo conformado por este organismo, cuyo propósito es proporcionar a los Estados miembros, una guía de orientación para la implementación de legislación, políticas, medidas tecnológicas e iniciativas adecuadas para combatir el Spam.

El *Anti-Spam Tool Kit* está compuesto de ocho elementos, que son:

- a) elementos regulatorios;
- b) medidas de ejecución;
- c) iniciativas de la industria;
- d) soluciones tecnológicas;
- e) educación y concientización;
- f) cooperación entre los distintos sectores;
- g) medidas anti-*Spam*; y
- h) cooperación global.

Los objetivos van encaminados a dar una respuesta internacional en las distintas políticas y a coordinar la lucha contra el Spam, alentado y promoviendo medidas, para combatir el Spam y códigos de buenas prácticas en el sector de la industria y negocio, así como facilitar la aplicación de las leyes fronterizas.

La OCDE ha llevado a cabo estudios referentes a delitos informáticos, en “1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de *ofrecer las bases para que los Estados y el sector privado, pudieran exigir un marco de seguridad para los sistemas informáticos.*”<sup>13</sup>

---

<sup>12</sup> Disponible en: [www.oecd-antispam.org](http://www.oecd-antispam.org), consultada el 01 de abril de 2011 a las 9:30 horas.

<sup>13</sup> Perea Quintana, Claudia Mireya, *Poder Judicial del Estado de Chihuahua*, México, año V, número 7, Supremo Tribunal de Justicia, 1999, p. 49.

- **El Foro para la Cooperación Asia-Pacífico (APEC).**<sup>14</sup>

México forma parte a través de la Secretaría de Economía, emitió en junio de 2005, los principios de acción en contra del Spam y sus guías de implementación para los 21 países miembros. Estos lineamientos buscan fomentar la cooperación internacional tomando como base lo que han hecho otros organismos internacionales, así como establecer mejores prácticas para su combate en la región Asia-Pacífico.

- **Unión Europea.**

El Spam Simposio 2007 tuvo lugar en Viena, Austria el 24 y 25 de mayo de 2007, que reunió a expertos europeos y de otros países, interesados en el análisis de la problemática del Spam y el *phishing* a nivel mundial, con la finalidad de encontrar soluciones viables para su combate.

En él se discutieron aspectos técnicos, jurídicos y regulatorios en materia de *phishing* y *Spam* (se abordaran más adelante), por ejemplo:

- a) la importancia de las leyes de privacidad y protección de datos como medios alternativos para contrarrestar el Spam y el *phishing* a nivel mundial;
- b) la evolución y el incremento de actividades en materia de crimen organizado;
- c) la coordinación de un mayor número de ISP (*Internet Service Provider*: Proveedor de Servicios de Internet);
- d) la cooperación internacional de las autoridades competentes encargadas de la persecución de *spammer's* a través de los organismos internacionales existentes.

Al igual se analizaron algunas de las técnicas que utilizan los *spammer's* para traspasar *software* y filtros anti-*Spam*, con objeto de acceder a las cuentas de

---

<sup>14</sup> Disponible en: [www.apec.org](http://www.apec.org) consultada el 01 de abril de 2011 a las 17:00 horas.

correo electrónico; los foros virtuales que utilizan para iniciarse en actividades *Spam* y compartir información sobre la disponibilidad de *botnets* (redes zombis), el acceso a servidores ubicados en países en vías de desarrollo, los principales productos que se comercializan a través del *Spam*, y los distintos métodos de pago que se usan para vender los productos al consumidor final (el término *spammer's* y *zombis* se analizará en el tercer capítulo).

- **Plan de Acción de la Cumbre Mundial sobre la Sociedad de la Información de Túnez (2005).**<sup>15</sup>

Negociada entre los años 2003 y 2005, esta declaración de los líderes mundiales hace un llamado a todas las partes interesadas a adoptar un enfoque multidimensional para contrarrestar el *Spam*, el cual incluye, entre otras cosas, la educación de los consumidores y de las empresas; una legislación, autoridades y herramientas adecuadas; el desarrollo continuo de medidas técnicas y de autorregulación; mejores prácticas; y cooperación internacional.

- **Unión Internacional de Telecomunicaciones de las Naciones Unidas (UIT).**<sup>16</sup>

Con base en la Resolución 50 de la Asamblea Mundial de Normalización de las Telecomunicaciones de 2004 la UIT, ha comenzado a trabajar en sus grupos de estudio, llevando a cabo investigaciones y actividades de intercambio de información para contribuir a los esfuerzos gubernamentales para frenar el *Spam*. De acuerdo con su mandato de desarrollar las telecomunicaciones, la UIT también ha proporcionado valiosos recursos sobre cómo lidiar con el *Spam* y otras amenazas relacionadas. También ha trabajado con el programa Infodev (*Information for Development Program: Información para Programas de Desarrollo*), del Banco Mundial para desarrollar un componente de las herramientas de reglamentación de la TIC (Tecnologías de la Información y la

---

<sup>15</sup> Disponible en: <http://www.itu.int/wsis/index-es.html>, consultada el 03 de abril del 2011 a las 10:00 horas.

<sup>16</sup> Disponible en: <http://www.itu.int/es/Pages/default.aspx>, consultada el 05 de abril 2011 a las 11:00 horas.

Comunicación), a veces se les conoce como NTIC (Nuevas Tecnologías de la Información y la Comunicación), para que se ocupe del problema del Spam.

Nota: En la presente investigación para hacer referencia al Spam, utilizaremos este mismo término, así como también, correo electrónico comercial no solicitado y/o correo electrónico no solicitado y/o mensaje electrónico no solicitado.

## CAPÍTULO II MARCO JURÍDICO.

### 2.1 Legislaciones ANTI-SPAM más importantes del mundo.

Al paso de los años han surgido varias legislaciones en torno al Spam y de las cuales daré una breve síntesis de los puntos más relevantes. Veremos que los legisladores aunque han identificado el problema, han promulgado leyes para restringirlos, no ha sido tarea fácil. Ya que las personas dedicadas al oficio del Spam encontraron nuevas conductas a modo de ocultar sus identidades, el claro ejemplo han sido las transmisiones abiertas, el falsificar sus direcciones, así como su correo electrónico. Es necesario ir más allá de cualquier conducta, para no dejar el paso a lagunas jurídicas y legales como veremos con las siguientes legislaciones:

#### a) ESTADOS UNIDOS DE AMÉRICA.

- CAN SPAM ACT.<sup>17</sup>

(Vigente desde el 16 de Diciembre del 2003). El acrónimo de CAN-SPAM se deriva del proyecto de ley *Controlling the Assault of No-Solicited Pornography and Marketing*. Promulgada por el Presidente George Bush el 16 de diciembre del 2003.

OBJETO: Es una Ley Federal que regula la transmisión de mensajes comerciales electrónicos no solicitados “Spam”.

En la promulgación de la ley se determinaron los siguientes puntos:

- ✓ Hay un interés importante del gobierno en la regulación del correo electrónico comercial a escala nacional.
  
- ✓ Los remitentes de correo electrónico comercial no debe inducir a error a los destinatarios en cuanto al origen o el contenido de este e-

---

<sup>17</sup> Can Spam Act 2003. (texto extraído, traducido y adaptado. Rodríguez García, Eric Ernesto), disponible en: <http://www.spamlaws.com/federal/108s877.shtml>, consultada el 23 de abril de 2011 a las 12:30 horas.

mail, es decir, los mensajes comerciales y mensajes electrónicos de transacción o relación no pueden contener la información del encabezado falsa o engañosa materialmente, y

- ✓ Los destinatarios de correo electrónico comercial tienen derecho a negarse a recibir más correo electrónico comercial de la misma fuente.

Además establece estándares para el control del SPAM, obliga a que los mensajes no solicitados estén bien etiquetados, que contengan el remitente, asunto y encabezado de correo, e incluir instrucciones para darse de baja, y otorga facultad a los ISP's (Internet Service Provider) para emprender acciones legales contra infractores, como se verá a continuación.

Esta ley no prohíbe el Spam, sólo establece requisitos para aquellos que envían correo electrónico comercial, fija sanciones para los spammer's y las empresas que anuncian productos en Spam, que violan la ley y ofrecen a los consumidores el derecho de pedir que se les deje de enviar Spam a sus correos.

Autoridades encargadas de hacer cumplir la ley:

- ✓ La Comisión Federal de Comercio (FTC) *Federal Trade Commission*.
- ✓ Departamento de Justicia (DOJ) *Department of Justice*, es encargado de cumplir las sanciones penales.
- ✓ Agencias federales y estatales, contra las organizaciones bajo su jurisdicción y las empresas que prestan "servicios de acceso a Internet" puede demandar a los infractores también.

Si bien es cierto, esta ley al ser creada por una potencia mundial, brindaría una protección y seguridad en cuanto al tema, la verdad es que no fue así, ya que solamente explica los términos en que debe realizarse el envío masivo de correos electrónicos de índole comercial.

Tienen que cumplirse una serie de condiciones para no infringir la ley, lo que significa que permitió que las personas responsables, aun sigan realizando sus actividades ilícitas, claro está, pero de una forma adecuada.

Esta ley no atacó directamente al Spam, es por ello que el Estado de California ha puesto su interés al crear una ley muy convincente, sus grandes opciones, para que se vea disminuido el porcentaje de envío de correo electrónico comercial no solicitado, son imponer sanciones realmente severas las cuales pueden alcanzar la cifra de un millón de dólares. Con esto creo que realmente se pensaría antes de infringir la ley, lo sorprendente de esto es que aunque quiera imponer sus sanciones, se ve frenada en su actuar por la CANSPAM.

## **b) ESPAÑA.**

- LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (vigente desde el 11 Julio 2002).

OBJETO: Regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios, incluidos los que actúen como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez, eficacia y el régimen

sancionador aplicable a los prestadores de servicios de la sociedad de la información<sup>18</sup>.

Son servicios de la sociedad de la información:

"Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información, comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios."

Se consideran servicios de la sociedad de la información, siempre y cuando representen una actividad económica los siguientes:

- ✓ La contratación de bienes o servicios por vía electrónica.
- ✓ La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.
- ✓ La gestión de compras en la red por grupos de personas.
- ✓ El envío de comunicaciones comerciales.
- ✓ El suministro de información por vía telemática.
- ✓ El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de suministro y recepción, y
- ✓ La distribución de contenidos previa petición individual.

Obligaciones establecidas en la ley:

- ✓ Para las empresas que realizan comercio electrónico: La ley se aplica al comercio electrónico y a otros servicios de Internet cuando sean parte de una actividad económica. Deben mostrar en su página web la siguiente información:

---

<sup>18</sup> Ley de servicios de la sociedad de la información y de comercio electrónico, disponible en: [http://noticias.juridicas.com/base\\_datos/Admin/l34-2002.t1.html#a1](http://noticias.juridicas.com/base_datos/Admin/l34-2002.t1.html#a1) consultada el 02 de mayo de 2011 a las 13:00 horas.

- \* Denominación social (NIF), domicilio y dirección de correo electrónico, teléfono o fax.
- \* Los datos de inscripción registral.
- \* Códigos de conducta a que estén adheridas.
- \* Precios de los productos o servicios que ofrecen, con indicación de los impuestos y gastos de envío.
- \* En su caso datos relativos a la autorización administrativa necesaria para el ejercicio de la actividad; datos de colegiación y título académico de profesionales que ejerzan una actividad regulada; e información adicional cuando el servicio se acceda mediante un número de teléfono de tarificación adicional.

En caso de realizar contratos on-line (en línea), se deberá añadir la siguiente información con carácter previo al contrato:

- \* Trámites que deben seguirse para contratar on-line,
- \* Si el documento electrónico se va a archivar y si éste será accesible,
- \* Medios técnicos para identificar y corregir errores en la introducción de datos,
- \* Lengua o lenguas en que podrá formalizarse el contrato,
- \* Condiciones generales a que, en su caso, se sujete el contrato, y
- \* Confirmar la celebración del contrato por vía electrónica, mediante el envío de acuse de recibido de pedido realizado.

✓ Para las empresas que hacen publicidad por vía electrónica:

- \* El anunciante debe identificarse claramente,
- \* El carácter publicitario del mensaje debe resultar inequívoco,
- \* Si se realizan ofertas, concursos o juegos promocionales, además de lo anterior, se deberá:
  - Identificar como tales, y

- Expresar de forma clara e inequívoca las condiciones de participación.
- \* Cuando se envíen por correo electrónico, mensaje SMS estos deberán:
  - Obtener con carácter previo la solicitud o autorización expresa del destinatario,
  - Identificar el mensaje publicitario con la palabra “publicidad” o la abreviatura “Publi.”, y
  - Establecer procedimientos sencillos para facilitar revocación de consentimiento del usuario.
- ✓ Para las empresas que prestan servicios de intermediación de la Sociedad de la Información. Los cuales son: operadores de telecomunicaciones; los proveedores de acceso a Internet (ISP’s); los prestadores de servicios de alojamiento de datos, enlaces y buscadores; deberán:
  - \* Colaborar con los órganos públicos para la ejecución de resoluciones que no puedan cumplirse sin su ayuda.
  - \* Informar a sus clientes sobre los diferentes medios técnicos que aumentan los niveles de seguridad de la información (anti-virus, anti-programas espía, filtros de correo); los aplicados por ellos; las herramientas existentes para el filtrado y restricción de acceso a determinados contenidos y servicios; y las posibles responsabilidades en que los usuarios pueden incurrir por el uso de Internet con fines ilícitos (ISP’s).

Responsabilidad:

- \* No son responsables de los contenidos que transmiten o alojan a los que facilitan acceso, si no participan en su elaboración.

- \* Son responsables si conocen su ilicitud y no actúa rápidamente para retirarlos o imposibilitar el acceso a ellos.
  
- ✓ Para los usuarios de Internet: Los titulares de las páginas personales, solamente si incluye publicidad, por la que perciban ingresos están sujetas a la Ley. En este caso:
  - \* Deben ofrecer información básica:
    - Nombre.
    - Residencia.
    - Dirección de correo electrónico.
    - Teléfono o fax.
    - NIF.
  
  - \* El anunciante debe identificarse claramente.
  - \* El carácter publicitario de la información debe resultar inequívoco.

Los derechos y garantías que se ofrecen en Internet gracias a esta Ley:

- ✓ Derecho a obtener información sobre los prestadores de servicios (nombre, domicilio, dirección de correo electrónico etc.), los precios de los productos o servicios que ofrecen, con la indicación de los impuestos y gastos de envío.
  
- ✓ Respecto a publicidad, derecho a conocer la identidad del anunciante, a no recibir mensajes promocionales no solicitados y a dejar de recibir los que hubiera autorizado.
  
- ✓ En la contratación, derecho a conocer los pasos necesarios para contratar por Internet, a acceder a las condiciones generales de la contratación antes de realizar su pedido y a obtener un acuse de

recibo del vendedor que le asegure que su pedido ha llegado al vendedor.

- ✓ Si el consumidor realiza una compra a través de Internet, además se beneficia del régimen de protección, que contempla la *“Ley de ordenación del comercio minorista para datos de las ventas a distancia.”*

Un país europeo sufre grandes consecuencias, ya que se ve afectado gravemente por la práctica sobre el correo electrónico comercial no solicitado, mejor conocido en España como: "comunicaciones comerciales enviadas por medios electrónicos", aunque este mismo es considerado como un delito y las sanciones a los responsables pueden alcanzar los 150 mil euros.

La ley permite dichos envíos sólo si el destinatario está de acuerdo en recibirlos, expresándolo mediante contrato, con la oportunidad de retractarse. De igual forma la empresa tiene la facultad de poder realizar estos actos de forma lícita, enviando publicidad comercial de sus productos, sólo si hay una relación formal entre cliente-consumidor.

Es de admirar el trabajo que viene realizando España, que si bien es cierto no ha logrado erradicar del todo, el problema del Spam, sí está haciendo todo lo posible, para no figurar en el top 10 de los principales países generadores de Spam, ya que estos resultados con los que aparecía hace seis años era muy preocupante, pues se encontraba situado dentro de los primeros cinco países en el mundo y primer lugar en Europa (algo que no le gustaría a ninguno), actualmente lo situaremos dentro del top 20, pero con un mínimo porcentaje.

### c) UNIÓN EUROPEA.

- LEY DIRECTIVA SOBRE LA PRIVACIDAD Y LAS COMUNICACIONES ELECTRÓNICAS.<sup>19</sup>(2002).

OBJETO: Las tecnologías de la información y la comunicación (TIC), en particular Internet y el correo electrónico, han de cumplir determinados requisitos para asegurar el derecho a la intimidad. La presente Directiva contiene normas esenciales destinadas a garantizar la confianza de los usuarios en los servicios y tecnologías de las comunicaciones electrónicas. Tales normas se centran en la prohibición de:

- 1) los mensajes electrónicos no solicitados (Spam),
- 2) el régimen de acuerdo previo del usuario (*opt-in*) y
- 3) la instalación de “chivatos” o *cookies*. “Javier Ribas Alejandro define *cookies* como: pequeños ficheros de datos que se generan a través de las instrucciones que los servidores web envían a los programas navegadores, y que se guardan en un directorio específico del ordenador del usuario.”<sup>20</sup>

Esta ley contiene normas destinadas a servir de marco al sector de las comunicaciones electrónicas. En ella se incluyen disposiciones sobre:

- ✓ la conservación de los datos de conexión por parte de los Estados miembros a efectos de vigilancia policial (retención de datos),
- ✓ el envío de mensajes electrónicos no solicitados, la utilización de los denominados *cookies*, y
- ✓ la inclusión de datos personales en las guías públicas.

---

<sup>19</sup> Ley Directiva sobre la Privacidad y las Comunicaciones Electrónicas (texto extraído, traducido y adaptado. Rodríguez García, Eric Ernesto), disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:es:NOT>, consultada el 31 de mayo de 2011 a las 14:00 horas.

<sup>20</sup> Ribas Alejandro, Francisco Javier, *Aspectos jurídicos del comercio electrónico en Internet*. Madrid, España, Aranzadí. 1999, p. 50.

El proveedor de un servicio de comunicaciones electrónicas está obligado a proteger la seguridad de sus servicios:

- ✓ garantizando que únicamente acceden a los datos de carácter personal las personas autorizadas;
- ✓ protegiendo los datos de carácter personal frente a su pérdida o alteración accidental;
- ✓ garantizando la aplicación de una política de seguridad relativa al tratamiento de datos de carácter personal.

Comunicaciones no solicitadas (spamming).

En relación con las comunicaciones electrónicas comerciales no solicitadas, la Directiva establece que los usuarios han de dar su consentimiento previo antes de recibir este tipo de mensajes (enfoque «**opt-in**»). Este sistema abarca asimismo los mensajes SMS (*short message Service*), son textos cortos de mensajería basada en telefonía móvil, y los demás mensajes electrónicos recibidos en cualquier equipo terminal, fijo o móvil. No obstante, se han establecido excepciones.

#### **d) ARGENTINA.**

- LEY DE PROTECCIÓN DE LOS DATOS PERSONALES (Octubre 2000).

OBJETO: la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las

personas, así como también el acceso a la información que sobre las mismas se registre (ART. 1)<sup>21</sup>.

Esta ley contiene normas sobre los principios generales de protección de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial habeas data, contenido en el artículo 43 de la Constitución de Argentina, ya que define y delimita aspectos fundamentales de la condición humana, en especial el derecho de acceder a su propia información, en caso de que no esté actualizada, sea falsa o discrimine, solicitar su debida actualización, ratificación, confidencialidad o en su caso supresión. Cubre además los datos contenidos en archivos, registros, bancos de datos u otros medios técnicos públicos y de protección de datos personales contenidos en archivos, registros, bancos de datos u otros medios técnicos privados.

Dentro de esta ley se contempla el derecho a la información, el cual consiste en que toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros (será de consulta pública y gratuita), bases o bancos de datos personales, sus finalidades y la identidad de sus responsables (art. 13).

Los requisitos que debe contener la información son los siguientes (art. 15):

- ✓ Se debe suministra en forma clara.
- ✓ Exenta de codificaciones.
- ✓ Acompañada de una explicación si se amerita.
- ✓ Lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.
- ✓ Amplia y versar sobre la totalidad del registro perteneciente al titular.
- ✓ No revelara datos pertenecientes a terceros.

---

<sup>21</sup> Ley de Protección de Datos Personales, disponible en: <http://www.red.org.ar/ley.htm>, consultada el 11 de junio de 2011 a las 11:00 horas.

- ✓ Será por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

Tendrán acceso a los archivos o bancos de datos por razones fundadas y cuando tengan competencia los siguientes Órganos (art. 18):

- ✓ Las Comisiones de Defensa Nacional.
- ✓ La Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación.
- ✓ La Comisión de Seguridad Interior de la Cámara de Diputados de la Nación o las que las sustituyan.

Sudamérica se ha visto invadido por un enorme virus denominado Spam, el problema era que en Argentina se le restaba la importancia necesaria y no se tomaron las medidas adecuadas para contrarrestar sus efectos, pero este país al igual que otros países como son Estados Unidos (por obvias razones), Corea del Sur, Brasil, China entre otros se encuentran en la lista de aquellos países, mismos que producían una cantidad muy alta y alarmante de correo electrónico comercial no solicitado, motivo por el cual surgió este ordenamiento.

Un dato a destacar es la resolución dictada por un juez en contra de varios spammer's por la práctica de este delito, la parte actora fueron dos licenciados que quisieron resolverlo de una manera normal, indicándole amablemente a la compañía responsable de dichos anuncios, que no les interesaban sus productos y por lo mismo les dejaron de enviar estos correos electrónicos, lo más lógico hubiese sido que lo dejarían de hacerlo, pero lo siguieron haciendo de una manera constante, hasta que los licenciados decidieran acudir ante la autoridad correspondiente, claro está que no fue una tarea nada fácil, el juez fue capaz de sancionar

estos actos al contar con una ley que respaldara sus decisiones al momento de emitir el fallo.

### Resolución contra el Spam

Cito el texto del Fallo del Juez Federal: Fdo. Roberto Raúl Torti:

“Buenos Aires, 11 de noviembre de 2003.

Agréguese, y en atención a lo solicitado, documentación acompañada y el derecho a la protección integral de los datos personales, garantizado por la ley 25.326, dispone que los aquí demandados se abstengan de seguir enviando mensajes de correo electrónico a las casillas de los actores y de transferir o ceder a terceros las direcciones de correo electrónico u otro dato personal vinculado a ellos (arts. 1, 2, 5, 11 y 27 de la ley citada), hasta tanto se resuelva el fondo de la cuestión.

Notifíqueme.

A fin de dar cumplimiento a lo previsto por el Art. 39 de la ley 25.326, córrase traslado a las demandadas por el plazo de cinco días, debiendo aportar la documentación pertinente. Notifíquese. Tiene presente la prueba ofrecida y la reserva del caso federal planteado.”<sup>22</sup>

Los spammer's realizan sus actividades por medio de listas muy extensas de direcciones de correos electrónicos (falta descubrir su autenticación), el dato que aporta esta ley es que si dicha base de datos de estos individuos proviene de un funcionario público aparte de la sanción a la que serán acreedores por infringir la ley, se les impondrá una inhabilitación de sus funciones hasta por cuatro años.

---

<sup>22</sup> Tanús, Gustavo Daniel disponible en: [www.protecciondedatos.com.ar](http://www.protecciondedatos.com.ar), consultada el 21 de junio de 2011 a las 18:00 horas.

## e) AUSTRALIA.

- SPAM ACT 2003 (entro en vigor el 10 de abril de 2004).

OBJETO: La Ley de Spam incluye normas destinadas a preservar legítimas actividades de comunicación empresarial y fomentar el uso responsable de la dirección electrónica de mensajería.<sup>23</sup>

De conformidad con esta Ley el envío del Spam es ilegal o hacer que se envíen, mensajes comerciales no solicitados de forma electrónica, incluyendo correo electrónico, mensajería instantánea, mensajes cortos o *SMS (short message service)* y *MMS (multimedia messaging system)* texto e imagen de mensajería basada en telefonía móvil. Las características que debe cubrir un mensaje comercial para que pueda ser enviado son las siguientes:

- ✓ Consentimiento: El mensaje debe ser enviado con consentimiento del destinatario.
- ✓ Identificar: Debe contener información precisa sobre la persona u organización que autorizó el envío del mensaje.
- ✓ Darse de baja: el mensaje debe contener una “unsubscribe”, facilidad para que el receptor pueda optar por no recibir mensajes de su organización.

Así mismo la Ley define a un mensaje comercial electrónico, como cualquier mensaje electrónico que:

- ✓ Ofrece, anuncia o promueve el suministro de bienes, servicios, terreno o negocio u oportunidades de inversión.
- ✓ Anuncia o promueve un proveedor de bienes, servicios, tierra o un proveedor de oportunidades de negocio o de inversión.
- ✓ Ayuda a una persona para obtener fraudulentamente la propiedad, obtener una ventaja comercial u otro beneficio de otra persona.

---

<sup>23</sup> Spam Act 2003 (texto extraído, traducido y adaptado. Rodríguez García, Eric Ernesto), disponible en: <http://www.comlaw.gov.au/Details/C2013C00021>, consultada el 17 de julio de 2011 a las 11:00 horas.

Se clasifica a un mensaje como comercial con base al:

- ✓ Contenido del mensaje.
- ✓ La forma en la que se presenta el mensaje.
- ✓ Todos los enlaces, números de teléfonos o información de contacto en el mensaje que llevan al contenido que tiene un fin comercial.

También se considera como mensaje comercial, cuando una empresa envía un mensaje de servicios, en él se incluye su dirección web, y en su sitio web incluyen actividades de promoción.

Uno de los requisitos *sine qua non* es el consentimiento de la persona a la cual se envía el mensaje, esta ley por su parte establece dos tipos de consentimiento:

- ✓ Expreso: El que puede adquirirse mediante la cumplimentación de un formulario, marcando una casilla que indique requerir publicidad en una página web, por teléfono, de forma personal, etc., siempre y cuando el destinatario este consiente de que se puede enviar publicidad en un futuro. Por tal motivo la empresa debe mantener un registro, ya que en caso de requerirse la autorización en la cual indique el consentimiento y la forma.
- ✓ Diferido: que a su vez se obtiene de dos formas:
  - \* Por medio de un negocio existente o de otro tipo, donde hay una expectativa razonable de recibir los mensajes electrónicos comerciales. Hay una relación comercial fuerte entre la organización y el titular de una dirección electrónica.
  - \* Cuando hay una relación con el trabajo, ejemplo cuando algún folleto o revista se relacione con el trabajo que desempeña la persona.

La autoridad responsable de sancionar y hacer cumplir la Ley de Spam, es ACMA: Comunicaciones de Australia y la Autoridad de Medios.

Muchos nos sorprenderíamos al ver los resultados obtenidos por este país, todo esto es gracias a que se puso un gran empeño para atacar este problema que nos afecta a todos. En verdad es de reconocer todo el trabajo que viene haciendo durante años, ya que realmente si se preocuparon en brindar una seguridad en el tema. Los spammer's en realidad lo van a dudar dos veces al realizar aquellas actividades cuando no existía un reglamento adecuado al cual se enfrentarían en caso de ser descubiertos, pero gracias a esta ley disminuyo drásticamente este tipo de problemas. Es importante mencionar que Australia antes de la creación de esta ley, formaba parte de los países con mayor porcentaje de correo electrónico comercial no solicitado.

Australia lo logró gracias a que las sanciones que impone son muy severas, no creo que nadie quiera ser sancionado por esta práctica, siendo acreedores de una multa de casi un millón de dólares australianos, pero es por cada mensaje enviado de esta manera. Algunos temas a destacar sobre la Ley, son que el remitente proporciona todos sus datos esenciales, con el fin que el destinatario decida si se da de baja para no seguir recibiendo dicha información, se necesita del consentimiento previo de los usuarios finales para enviar correo electrónico comercial no solicitado.

#### **f) Países con legislación Anti-Spam.**

Muchos países preocupados por la situación que representa el correo electrónico comercial no solicitado, se dieron en la tarea de la creación de leyes, para poder dar una solución a los usuarios en el Internet, los cuales somos los principales afectados, ya que nosotros recibimos los ataques.

Existen datos los cuales muestran a los primeros países en realizar legislaciones Anti-Spam, los cuales son Holanda y Malasia cuyas legislaciones fueron creadas en el año 1998. Al paso del tiempo y más afectaciones del Spam, fueron apareciendo nuevas legislaciones en cuestión, inclusive la gran potencia mundial y me refiero a los Estados Unidos incluyeron su ley.

A continuación mostrare las legislaciones que regulan al correo electrónico comercial no solicitado alrededor del mundo.

<b>PAÍS</b>	<b>LEGISLACIÓN</b>	<b>ÁREA</b>	<b>VIGENCIA</b>
<b>ARGENTINA</b>	Ley de protección de datos.	Protección de Datos.	2000
<b>AUSTRIA</b>	<i>Federal act concerning the protection of personal data.</i>	Protección de Datos.	1999
<b>AUSTRALIA</b>	<i>Spam Act.</i>	E-mail; SMS; Mensajes comerciales electrónicos; Se excluyen las llamadas masivas, no son consideradas	<b>2005</b>

		mensajes comerciales electrónicos.	
<b>BÉLGICA</b>	<i>Loi sur certains aspects juridiques des services de la société de l'information.</i>	Mensajes electrónicos; Protección de Datos.	2003
<b>BRASIL</b>	Movimiento brasileño de combate.	Protección de Datos.	<b>2008</b>
<b>CANADÁ</b>	<i>Personal information protection and electronic documents act.</i>	Protección De Datos.	2000
<b>CHILE</b>	Ley del consumidor.	E-mail.	2004
<b>COLOMBIA</b>	Protección de datos.	E-mail.	<b>2008</b>

<b>PAÍS</b>	<b>LEGISLACIÓN</b>	<b>ÁREA</b>	<b>VIGENCIA</b>
<b>COSTA RICA</b>	Reglamento autónomo de servicio para la regulación del correo electrónico masivo o no deseado.	E-mail.	2002
<b>DINAMARCA</b>	<i>The marketing practices Act.</i>	E-mail.	<b>2005</b>
<b>ECUADOR</b>	Ley de comercio electrónico, firmas electrónicas y mensajes de datos.	E-mail.	2002
<b>ESPAÑA</b>	Ley de servicios de la sociedad de la información y de comercio electrónico.	E-mail.	2002
<b>ESTADOS UNIDOS</b>	<i>Can Spam Act.</i>	E-mail; SMS (tipo De mensajería).	2003

<b>PAÍS</b>	<b>LEGISLACIÓN</b>	<b>ÁREA</b>	<b>VIGENCIA</b>
<b>FINLANDIA</b>	<i>Act on data protection in electronic communications.</i>	Protección De Datos.	2004
<b>FRANCIA</b>	<i>Pour la confiance dans l'économie numérique.</i>	E-mail.	2004
<b>HOLANDA</b>	<i>Dutch telecommunications Act.</i>	Telecomunicaciones.	1998
<b>ITALIA</b>	<i>Data protection code.</i>	E-mail; Facsímile; MMS/SMS (tipo de mensajes); Protección de datos.	2003
<b>INDIA</b>	Coalición contra el correo electrónico no solicitado.	E-mail.	<b>2008</b>

<b>PAÍS</b>	<b>LEGISLACIÓN</b>	<b>ÁREA</b>	<b>VIGENCIA</b>
<b>JAPÓN</b>	Ley de ordenación del transporte de correo electrónico específico.	E-mail.	2002.
<b>LITUANIA</b>	Ley de comunicaciones electrónicas.	PROTECCIÓN DE DATOS.	2004
<b>MALASIA</b>	<i>Communications and multimedia Act.</i>	E-mail; Servicio postal; Comunicaciones Multimedia.	1998
<b>MALTA</b>	Protección de datos.	Protección de datos.	2003
<b>NORUEGA</b>	<i>The marketing control Act.</i>	Protección de datos Electrónicos; E-mail; Telefax; MMS/SMS (tipo de mensajes).	<b>2006</b>

<b>PAÍS</b>	<b>LEGISLACIÓN</b>	<b>ÁREA</b>	<b>VIGENCIA</b>
<b>PERÚ</b>	Ley que regula el envío de correo electrónico comercial no solicitado.	E-mail.	<b>2005</b>
<b>POLONIA</b>	Ley de telecomunicaciones.	Protección de datos.	2004
<b>PORTUGAL</b>	Decreto ley 7/2004.	Protección de datos.	2004
<b>REPÚBLICA DE COREA</b>	Ley de promoción de la información y la utilización de comunicaciones de red y de protección de datos.	Protección de datos.	2001
<b>REPÚBLICA POPULAR CHINA</b>	Reglamento de servicios de email por internet.	E-mail.	<b>2006</b>

<b>PAÍS</b>	<b>LEGISLACIÓN</b>	<b>ÁREA</b>	<b>VIGENCIA</b>
<b>REINO UNIDO</b>	La privacidad y las comunicaciones electrónicas.	Protección de datos.	2003
<b>RUSIA</b>	Código civil de Rusia (modifica su art. 309).	Protección de datos.	<b>2006</b>
<b>SINGAPUR</b>	<i>Proposed Spam control bill.</i>	E-mail; MMS/SMS (tipo de mensajes)	<b>2005</b>
<b>UNIÓN EUROPEA</b>	Ley directiva sobre la privacidad y las comunicaciones electrónicas.	E-mail; SMS (tipo De mensajería).	2002
<b>VENEZUELA</b>	Ley especial contra delitos informáticos.	E-mail.	2001

## 2.2 Problemática legal en México.

### 2.2.1 Constitución Política de los Estados Unidos Mexicanos.<sup>24</sup>

#### A) Libertad de expresión:

*“Artículo 6o.- La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.*

*Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:*

*I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.*

*II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*

*III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.*

*IV. Se establecerán mecanismos de acceso a la información y*

---

<sup>24</sup> Constitución Política de Los Estados Unidos Mexicanos, 27ª. ed., México, Ediciones Fiscales Isef, 2012.

*procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.*

*V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.*

*VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.*

*VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.”*

**B) Libertad de imprenta:**

*“Artículo 7o.- Es inviolable la libertad de escribir y publicar escritos sobre cualquiera materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública. En ningún caso podrá secuestrarse la imprenta como instrumento del delito.*

*Las leyes orgánicas dictarán cuantas disposiciones sean necesarias para evitar que so pretexto de las denuncias por delitos de prensa, sean encarcelados los expendedores, "papeleros", operarios y demás empleados del establecimiento donde haya salido el escrito denunciado, a menos que se demuestre previamente la responsabilidad de aquéllos”.*

**C) Principio de legalidad.**

*“Artículo 14. A ninguna ley se dará efecto retroactivo en perjuicio de persona alguna.*

*Nadie podrá ser privado de la libertad o de sus propiedades, posesiones o derechos, sino mediante juicio seguido ante los tribunales previamente establecidos, en el que se cumplan las formalidades esenciales del procedimiento y conforme a las Leyes expedidas con anterioridad al hecho.”*

*“En los juicios del orden criminal queda prohibido imponer, por simple analogía, y aún por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito de que se trata.*

*En los juicios del orden civil, la sentencia definitiva deberá ser conforme a la letra o a la interpretación jurídica de la ley, y a falta de ésta se fundará en los principios generales del derecho.”*

**D) Garantía de seguridad jurídica.**

*“Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.*

*Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.*

*No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querrela de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.*

*La autoridad que ejecute una orden judicial de aprehensión, deberá poner al inculpado a disposición del juez, sin dilación alguna y bajo su más estricta responsabilidad. La contravención a lo anterior será sancionada por la ley penal.*

*Cualquier persona puede detener al indiciado en el momento en que esté cometiendo un delito o inmediatamente después de haberlo cometido, poniéndolo sin demora a disposición de la autoridad más cercana y ésta con la misma prontitud, a la del Ministerio Público. Existirá un registro inmediato de la detención.*

*Sólo en casos urgentes, cuando se trate de delito grave así calificado por la ley y ante el riesgo fundado de que el indiciado pueda sustraerse a la acción de la justicia, siempre y cuando no se pueda ocurrir ante la autoridad judicial por razón de la hora, lugar o circunstancia, el Ministerio Público podrá, bajo su responsabilidad, ordenar su detención, fundando y expresando los indicios que motiven su proceder.*

*En casos de urgencia o flagrancia, el juez que reciba la consignación del detenido deberá inmediatamente ratificar la detención o decretar la libertad con las reservas de ley.*

*La autoridad judicial, a petición del Ministerio Público y tratándose de delitos de delincuencia organizada, podrá decretar el arraigo de una*

*persona, con las modalidades de lugar y tiempo que la ley señale, sin que pueda exceder de cuarenta días, siempre que sea necesario para el éxito de la investigación, la protección de personas o bienes jurídicos, o cuando exista riesgo fundado de que el inculpado se sustraiga a la acción de la justicia. Este plazo podrá prorrogarse, siempre y cuando el Ministerio Público acredite que subsisten las causas que le dieron origen. En todo caso, la duración total del arraigo no podrá exceder los ochenta días.*

*Por delincuencia organizada se entiende una organización de hecho de tres o más personas, para cometer delitos en forma permanente o reiterada, en los términos de la ley de la materia.*

*Ningún indiciado podrá ser retenido por el Ministerio Público por más de cuarenta y ocho horas, plazo en que deberá ordenarse su libertad o ponérsele a disposición de la autoridad judicial; este plazo podrá duplicarse en aquellos casos que la ley prevea como delincuencia organizada. Todo abuso a lo anteriormente dispuesto será sancionado por la ley penal.*

*En toda orden de cateo, que sólo la autoridad judicial podrá expedir, a solicitud del Ministerio Público, se expresará el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan, a lo que únicamente debe limitarse la diligencia, levantándose al concluirla, un acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o en su ausencia o negativa, por la autoridad que practique la diligencia.*

*Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno*

*de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.*

*Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración.”*

*La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.*

*Los Poderes Judiciales contarán con jueces de control que resolverán, en forma inmediata, y por cualquier medio, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación de la autoridad, que requieran control judicial, garantizando los derechos de los indiciados y de las víctimas u ofendidos. Deberá existir un registro fehaciente de todas las comunicaciones entre jueces y Ministerio Público y demás autoridades competentes.*

*Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio.*

*La autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos*

*sanitarios y de policía; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetándose en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos.*

*La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley.*

*En tiempo de paz ningún miembro del Ejército podrá alojarse en casa particular contra la voluntad del dueño, ni imponer prestación alguna. En tiempo de guerra los militares podrán exigir alojamiento, bagajes, alimentos y otras prestaciones, en los términos que establezca la ley marcial correspondiente.”*

### **2.2.2 Código Penal Federal.<sup>25</sup>**

**CAPÍTULO II. Acceso ilícito a sistemas y equipos de informática. (Artículo 211- BIS.1 AL 211-BIS.7).** En este apartado del código se hace alusión a las diferentes acciones realizadas por algún sujeto, el cual tenga o no la autorización para acceder a información importante y valiosa, misma que se puede encontrar en los diferentes equipos de cómputo, es decir, ya sean propiedad del Estado o de los particulares y que por lo tanto puede ser destruida, alterada o modificada siendo estos mismos, acreedores a una sanción determinada por su manera de actuar.

### **2.2.3 Ley de Datos Personales en Posesión de los Particulares.<sup>26</sup>**

De manera general la presente Ley tiene como función primordial, el brindar protección a las personas, que depositan sus datos confidenciales en manos de

---

<sup>25</sup> Código Penal Federal, 12ª. ed., México, Sista, 2012.

<sup>26</sup> Disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>, consultada el 13 de agosto de 2011 a las 13:00 horas.

particulares, esto sucede a través de bancos, escuelas, hospitales, etc., a las cuales brindamos información personal necesaria, la cual es almacenada en una base de datos, de todos los sujetos existentes, para que estos mismos puedan ser identificados en algún momento determinado y tengamos la confianza de que esta misma institución va a salvaguardar aquella información en todo momento.

#### **2.2.4 Ley Federal de Protección al Consumidor.**

En lo que respecta a la presente ley se habla de que las empresas no molesten con publicidad en nuestros domicilios, centros de trabajo de forma personal, telefónica, por correo electrónico o por cualquier otro medio, con el objetivo de vender u ofrecer sus servicios, bienes o productos, es tarea que concierne a la Procuraduría Federal del Consumidor (PROFECO) dependencia encargada de proteger al consumidor. Es por ello que se muestra muy interesado en combatir uno de los principales problemas que hoy día afectan al consumidor, que es el envío de Spam, colaboro en el año 2003 con países que son miembros del Comité de políticas del consumidor (CCP) en la elaboración “*Background Paper on Spam*”, documento en donde se realiza un análisis del Spam y las empresas auxiliándose de cuerpos legales y normativos puedan combatirlo.

Así que abocándose a su tarea decidió reformar su Ley, que aunque ya contemplaba las operaciones a través de medios electrónicos, aun desprotegía a las autoridades y ciudadanos, en comunicaciones vía electrónica y publicidad no deseada.

El 4 de febrero del 2004 se reformó y modificó la **Ley Federal de Protección al Consumidor**<sup>27</sup>, en su artículo 17, 18 y 18 BIS. Quedando de la siguiente forma:

---

<sup>27</sup> Ley Federal de Protección al Consumidor, disponible en: [http://www.profeco.gob.mx/juridico/pdf/l\\_lfpc\\_ultimo\\_camDip.pdf](http://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_camDip.pdf), consultada el 01 septiembre de 2011 a las 10:30 horas.

**“Art. 17.-** En la publicidad que se envíe a los consumidores se deberá **indicar el nombre, domicilio, teléfono** y, en su defecto, la **dirección electrónica del proveedor**; de la **empresa** que, en su caso, envíe la publicidad a **nombre del proveedor, y de la Procuraduría**.

El consumidor podrá exigir directamente a proveedores específicos y a empresas que **utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica** o por cualquier otro medio, para **ofrecerle bienes, productos o servicios**, y que **no le envíen publicidad**. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con **finés mercadotécnicos o publicitarios**, que **la información** relativa a él mismo **no sea cedida o transmitida** a terceros, salvo que dicha cesión o transmisión sea determinada por una **autoridad judicial**.”

**“Art. 18.-** La **Procuraduría** podrá llevar, en su caso, un **registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios**. Los consumidores podrán comunicar **por escrito o por correo electrónico** a la **Procuraduría** su solicitud de inscripción en dicho registro, el cual será **gratuito**.”

**“Art. 18 BIS.-** Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el artículo anterior. Los proveedores que

*sean objeto de publicidad son corresponsables del manejo de la información de consumidores cuando dicha publicidad la **envíen a través de terceros.***”

Como podemos ver la Ley Federal de Protección al Consumidor no difiere mucho de la legislación Internacional, ya que se establece:

1. Identificación de la Empresa o Proveedor: La empresa se identifique en el momento de enviar la publicidad a los consumidores indicando:
  - Nombre.
  - Domicilio.
  - Teléfono.
  - En su defecto la dirección electrónica del proveedor.
2. Derecho del consumidor: Podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad.

**Confidencialidad:** la información del consumidor no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.

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

4. Responsabilidad de los proveedores: Los proveedores que sean objeto de publicidad son corresponsables del manejo de la información de consumidores, cuando dicha publicidad la envíen a través de terceros.

Aunque la PROFECO cumplió al brindar protección al consumidor, no ha logrado del todo que el envío de correo no solicitado se frene totalmente, es necesario que se realice conciencia sobre el buen uso del Internet, y que tanto las empresas, como los proveedores dedicados a la mercadotecnia y publicidad sean responsables y cumplan con las normas establecidas.

Es necesario que la legislación mexicana existente cuente con mayor cobertura en cuanto al tema del SPAM, pues no sólo se trata del no envío de mensaje no solicitado, sino especificar de forma adecuada y precisar el SPAM, de que se trata, pero asimismo ser específico en cuanto a las sanciones y penalidades, pues no es lo mismo hablar de simple publicidad, a que se hable de un Spam que cause daño, a nuestro hardware a raíz de que se envió la publicidad. O en el peor de los casos que nuestros datos queden expuestos al criterio de terceras personas y se afecte con ello nuestro patrimonio.

## CAPÍTULO III. MARCO CONCEPTUAL.

### 3.1 Campo de estudio del Derecho Informático.

Desde que apareció la informática en la vida diaria del hombre a la par surgieron problemáticas, de la cual el derecho no podía estar ajeno y en su intento por resolverlas, surge el derecho informático. Para comprender el significado del derecho informático, se necesita dar el primer concepto base de esta tesis; la informática “proviene del termino información y del vocablo automático, cuyas raíces provienen de las bases griegas << *authos*>>, que significa uno mismo, << *mathoma*>>, que se traduce como lanzarse, por lo que se entiende por automático a aquello que se lanza o activa por sí mismo.”<sup>28</sup>

Por lo que la informática supone el procesamiento automático de la información. Si el Derecho se encarga del comportamiento humano en sociedad, por tanto debe de estudiar el comportamiento del mismo ante los cambios tecnológicos y su interacción.

Para Hermilio Tomás Azpilcueta el derecho de la informática:

“Concierne a los aspectos jurídicos de la memorización y al tratamiento de las informaciones.”<sup>29</sup>

Por su parte Julio Téllez Valdés nos da el siguiente concepto de informática:

“Es la rama de las ciencias jurídicas que considera la informática como instrumento (informática jurídica) y objeto de estudio (derecho de la informática).”<sup>30</sup>

---

<sup>28</sup> F. Kuhlmann, A. Alonso, Información y telecomunicaciones, México, Fondo de cultura económica, 1996, p. 11.

<sup>29</sup> Tomás Azpilcueta, Hermilio, *Derecho informático*, Buenos Aires, Argentina, Abeledo- Perrot, 1987, p. 45.

<sup>30</sup> Téllez Valdés, Julio, op. cit., nota 1, p. 17.

El mismo autor al desglosar el anterior concepto divide para su estudio en:

“Informática jurídica o Jurísmatica, es la técnica interdisciplinaria que estudia e investiga la informática general aplicable a la recuperación de análisis y tratamientos jurídicos.”<sup>31</sup>

“Derecho de la informática es el conjunto de leyes, normas y principios aplicables a hechos y actos derivados de la informática.”<sup>32</sup>

Con las anteriores definiciones podemos deducir que el Derecho Informático es la rama de las ciencias jurídicas que considera la informática como instrumento, se encarga del estudio e investigación de la informática en general aplicable a la recuperación de análisis y tratamientos jurídicos; y como objeto de estudio, es el conjunto de leyes, normas y principios aplicables a hechos y actos derivados de la informática.

A su vez la informática jurídica se divide para su estudio en:

- a) Informática jurídica documentaria: se evoca en crear y recuperar datos de carácter jurídico de los cuales encontramos a la ley, la jurisprudencia, la doctrina u otros datos de interés jurídico y legal. Estos documentos conforman los bancos de datos jurídicos.
- b) Informática jurídica de gestión: “es la dedicada de una u otra forma a la mecánica de la oficina jurídica, en el más amplio sentido de la palabra.”<sup>33</sup>

Para su estudio se divide en tres grupos:

- Informática registral: se lleva a cabo un registro tanto de carácter público como privado.

---

<sup>31</sup> Ibídem, p. 19.

<sup>32</sup> Ibídem, p. 21.

<sup>33</sup> Tomás Azpilcueta, Hermilio, op. cit., nota 29, p. 53.

Su objetivo es que se ingrese con facilidad, rapidez, y de forma instantánea desde cualquier oficina pública, mediante el pago para el ingreso a los sistemas de control y reserva de datos por ejemplo, al registro civil, al registro de la propiedad intelectual e industrial, entre otros.

- Informática operacional: ayuda al sector público y privado en las actuaciones de la oficina relacionadas con el derecho, por ejemplo, a nivel público en la actividad del juzgado la máquina llevara todas las actuaciones de las fases del proceso, etc. En tanto que en el sector privado en lo que se refiere a los bufetes o despachos de abogados servirá para el control de pleitos, contabilidad y demás.
  - Informática decisional: ayuda al juez a establecer determinadas pautas en resoluciones muy repetitivas así que facilita la redacción de la misma, utilizando un formato preestablecido, en donde solo se agregan los datos variables que aporta el juez en la computadora para posteriormente imprimir la resolución íntegra, por ejemplo, sentencia de separación y divorcio de común acuerdo, sentencias de remate, entre otros.
- c) Informática jurídica de ayuda a la difusión o metadecisional: "... todas las actividades, trabajos y distintas aplicaciones de las máquinas de computación, en sus múltiples manifestaciones, con motivo de la memorización y tratamiento de la información, genera efectos y relaciones jurídicas, que, en su conjunto, conforman el derecho informático.<sup>34</sup>"

En esta área de la informática lo que se trata es, lograr que la computadora auxilie a ayudar al jurista a resolver los problemas jurídicos en los tres tradicionales campos de legislación, jurisprudencia y bibliografía.

---

<sup>34</sup> Ibidem, p. 56.

Ahora bien, el derecho a la informática se divide para su estudio:

a) Política informática: tiene que ver con los procesos de manejo de la información, es de observancia general y obligatoria para las dependencias y entidades de gobierno del estado, por ello crean normas para una política informática adecuada. De acuerdo con el autor Julio Téllez Valdés, algunos puntos importantes propuestos para la política informática son:

- Adecuado desarrollo de la industria de construcción de equipos de cómputo y de programación.
- Planeación, difusión y aplicación del fenómeno informático.
- Contratación gubernamental de bienes y servicios informáticos.
- Formulación de normas y estándares en materia informática.
- Control de importaciones y exportaciones sobre equipos, accesorios y programas de computadoras.

b) Legislación informática: conjunto de reglas de carácter preventivo y correctivo derivadas del uso de la informática. Las cuales se consideran en la creación de nuevas leyes de carácter específico. Las reglas que se deberán tomar en cuenta son las siguientes:

- Regulación de los bienes informativos.
- Protección de datos personales.
- Regulación jurídica de Internet.
- Propiedad intelectual e informática.
- Delitos informáticos.
- Contratos informáticos y firma digital.
- Comercio electrónico.
- Aspectos laborales de la informática.
- Valor probatorio de los soportes modernos de la información.
- Correo electrónico, privacidad, en ella ubicamos al Spam.
- Cómputo forense.

### c) Problemas del correo electrónico.

Los diferentes problemas que presentan los correos electrónicos se relacionan con las dificultades que se plantean en los servidores, estas consisten en:

- “Backdoor (puerta trasera): secuencia especial del código de programación que usa el programador para acceder o escapar en caso de emergencia. Terceras personas pueden utilizarlo con fines maliciosos y/o espionaje.
- Bug: error o defecto de *software*, estos pueden actuar como <<puertas traseras>> para los *hackers*.
- Exploit (explotar): forma de automatizar el aprovechamiento de un error o de un fallo para causar un comportamiento no deseado.
- Malware: *Software* dañino. Engloba virus, troyanos, automarcadores, *spyware* (espías), *adware* (programas publicitarios), *keyloggers* (secuestra claves), etc.
- Hoax (bulo): correo con contenido falso y atrayente. Se suele distribuir en cadena para captar direcciones de correo electrónico, revelar contraseñas o instalar *malware* (virus, troyanos, etc.).
- Troyano: programa que lleva en su interior un programa malicioso o un virus.
- Ataque de denegación de servicios: bombardeo de mensajes que provoca una respuesta del servidor, saturando al servidor e incluso dejándolo inaccesible durante un tiempo.

- Spam: mensajes no solicitados, normalmente de publicidad y enviados en gran cantidad de gente a la vez. Muchos proveedores de correo ya consideran Spam los mensajes para unos pocos usuarios, otros usan listas etc.”<sup>35</sup>
- Phishing: delito tipo estafa para conseguir, de forma fraudulenta y con <<ingeniería social>> (engaños o suplantación de personalidad) información confidencial (contraseñas, cuentas o tarjetas bancarias, etc.)<sup>36</sup>
- Delito Informático: *“aquel que tipifica cualquier acto humano como ilegal cuando dicho acto tiene como finalidad afectar datos, información o sistemas de información cuya consecuencia sea el daño directo o indirecto entre ellos así como el mal uso de estos.”*<sup>37</sup>

### 3.2 Definición del SPAM.

Como se ha visto, el Spam no significa cualquier cosa, representa no sólo una molestia atacarlo, además incluye perdidas tanto económicas como materiales, ahora bien, es responsabilidad de los usuarios y el gobierno poner atención a todas las anomalías que se están realizando impunemente. La problemática a tratar en este capítulo, es dar una definición clara sobre el Spam y posteriormente entender este fenómeno en su totalidad, así como el alcance que llega a tener, en todos los aspectos, pero destacando la gravedad ocasionada. Muchos autores dan una idea general sobre la concepción del Spam, al igual que

<sup>35</sup> Andreu Gómez, Joaquín, *Servicios en red, informática y comunicaciones*, Madrid, España, Editex, 2010, p. 120.

<sup>36</sup> Esta modalidad de fraude es un poco más actual, su modo de operar es hacerle creer al usuario o receptor final, que es de vital importancia actualizar sus datos bancarios. La información nos llega de la misma manera por correo electrónico, el cual menciona dicha información, junto con un link que nos dirige a un sitio web supuestamente oficial de nuestra sucursal bancaria.

El propósito es brindar nuestros datos confidenciales de la cuenta bancaria, ya sean contraseñas, números de cuenta, nosotros al pensar que estamos en un sitio confiable lo haremos, porque nos presionan diciendo que si no se realizan o confirman dichos cambios nos cobrarán en un futuro o hasta se cancelara dicha cuenta.

El verdadero problema surge después ya que aparte de perder ese depósito que realizamos, podrán tener libre acceso a nuestra cuenta e incluso robarán nuestra identidad.

<sup>37</sup> Muñoz Torres, Ivonne Valeria, *Delitos informáticos*, México, Ubijus, 2009, p. 19.

algunos sitios web, en donde se considera en resumen como los: Mensajes no solicitados, con remitente desconocido, de carácter publicitario, enviado en cantidades masivas, logrando perjudicar de varias formas al receptor, y que tiene por fin el ánimo de lucro.

Algunas definiciones sobre el término Spam son las siguientes:

“Envió masivo, indiscriminado y no solicitado de publicidad a través de correo electrónico.”<sup>38</sup>

“Envió masivo –y a veces repetido- de correos electrónicos no solicitados, generalmente de carácter comercial, dirigidos a personas con las que el remitente no ha tenido nunca contacto alguno que ha recogido la dirección electrónica de espacios públicos en Internet: foros de discusión, listas de distribución, anuarios, sitios web, etc.”<sup>39</sup>

“Cualquier mensaje por correo electrónico que sea transmitido en forma no solicitada a un gran número de receptores.”<sup>40</sup>

“... se realiza a través de correo electrónico; es un correo no solicitado por su receptor, su contenido carece de utilidad, puede ser ilegal, o bien es información o publicidad que no es de interés de su receptor; la dirección del destinatario no ha sido recogida de forma legal y no se ha solicitado su consentimiento.”<sup>41</sup>

“El Spam se refiere sólo a las comunicaciones publicitarias no solicitadas a través de medios electrónicos, y advierte que otras formas de comunicaciones no deseadas son el *junk mail*, que no

---

<sup>38</sup> Téllez Valdés, Julio, op. cit., nota 1, p. 497.

<sup>39</sup> Messía de la Cerda Ballesteros, Jesús Alberto, *La protección de datos de carácter personal en las telecomunicaciones*, España, Madrid, DYKINSON, S. L., 2004, p. 178.

<sup>40</sup> Sánchez del Castillo, Vilma, *La publicidad en internet: Régimen jurídico de las comunicaciones electrónicas*, La ley, Grupo Wolters Kluwer, 2007, p. 326.

<sup>41</sup> Ídem.

necesariamente tiene una finalidad comercial y el *mail bombing*, que es el que intencionalmente se envía para bloquear una cuenta de correo electrónico.”<sup>42</sup>

“...como el correo solicitado, que mayoritariamente, pero no siempre se ha enviado con fines publicitarios.”<sup>43</sup>

“... La variedad del contenido de los mensajes calificados como UCE pueden pulular entre lo inofensivo, lo ofensivo y lo falso, por ello la cuestión no debe rondar sobre los beneficios del medio que transporta esas comunicaciones, sino más bien en determinar si los beneficios de ese canal de expresión comercial, requiere de intervención y el control del gobierno.”<sup>44</sup>

“Se considera Spam al ataque a la privacidad caracterizada por la invasión indiscriminada y no autorizada al correo electrónico de una persona física o jurídica, por medio del envío de mails publicitarios o de cualquier otro tipo.”<sup>45</sup>

“... consiste en obtener listas de direcciones de correo a través de empresas que se dedican a recopilarlas y venderlas, y enviar correos con publicidad e incluso virus a personas que ni lo han solicitado ni autorizado.”<sup>46</sup> Dichos autores dan su concepto de Spam, algunos de ellos aunque ya sea que mencionen o no, los elementos que lo distinguen siempre parten de una idea general, por lo tanto, para mí la definición idónea de Spam es:

---

<sup>42</sup> Sánchez del Castillo, Vilma, op. cit., nota 40, p.4.

<sup>43</sup> Ibídem, p. 327.

<sup>44</sup> Ídem.

<sup>45</sup> Cárpoli, Gabriel Andrés, *Derecho penal informático en México*, México, Instituto Nacional de Ciencias Penales, INACIPE, 2004, p. 69.

<sup>46</sup> Cursos de Informática aulalic.es. disponible en: <http://books.google.com.mx/books?id=cXUJDjScRNUC&pg=PA135&dq=spam&hl=es-419&sa=X&ei=A334UKTXLPC62gXD14CAA&ved=0CEgQ6AEwBDgU#v=onepage&q=spam&f=false>, consultada el 15 de noviembre de 2011 a las 12:00 horas.

“Toda aquella información que no hemos solicitado, pero que se recibe por cualquier medio electrónico e informático, no sólo de carácter publicitario, sino de cualquier índole, engañándonos al ser dirigidos a sitios web falsos, para la obtención de datos confidenciales a terceros, con ánimos de lucro.”

Como podemos darnos cuenta al recibir un mensaje electrónico de las características anteriores, tendremos que lidiar con acciones fraudulentas, información falsa, virus (*malware*), para nuestras computadoras, incluso si no somos cuidadosos al respecto perderemos nuestro tiempo y dinero.

### 3.3 Sujeto activo del Spam.

Es aquel individuo que sobresale de los demás por su talento en el manejo de sistemas operativos. Los sujetos activos principales en los ilícitos informáticos son:

- **Hacker:**

- ✓ “Es un término empleado para identificar indistintamente a un “programador habilidoso”, o bien, a un “allanador de sistemas informáticos que altera programas.”<sup>47</sup>
- ✓ Para los autores Orts Berebguer, Enrique y Roig Torres, Margarita el hacker es: “...aquellas personas expertas en informática que entran en otras máquinas por razones exclusivamente educativas o de diversión, mientras que los intrusos con intenciones criminales o vandálicas tendrían reservado el término cracker.”<sup>48</sup>

---

<sup>47</sup> Molina Salgado, José Antonio, *Breviarios jurídicos. Delitos y otros ilícitos informáticos en el derecho de la propiedad industrial*, México, Porrúa, 2003, p. 17.

<sup>48</sup> Azaola Calderón, Luis, *Delitos informáticos y Derecho Penal*, México, Ubijus, 2010, p. 31.

Concluyo que el hacker, es aquel individuo que tiene habilidades en el manejo de la computadora, capaz de acceder, introducirse o romper, la seguridad de un sistema informático ajeno.

- **Crackers:**

- ✓ “Es una persona que intenta acceder a un sistema informático sin autorización. Estas personas tienen a menudo malas intenciones, en contraste con los hackers, y pueden disponer de muchos medios para introducirse en un sistema.”<sup>49</sup>
- ✓ Al respecto Moránt Vidal J. Los Crackers da la siguiente definición: “...son los piratas informáticos, personas que se introducen en sistemas remotos con la intención de destruir datos, de negar el servicio a usuarios legítimos”, y en general a causar problemas, pudiéndose apreciar dos variantes de los mismos:
- ✓ El que penetra en un sistema informático y roba información o provoca destrozos en el mismo.
- ✓ El que se dedica a desproteger todo tipo de programas, tanto de versiones shareware (programas limitados a modo de prueba), para hacerlas plenamente operativas, como de programas completos comerciales que presentan protecciones anti copia.”<sup>50</sup>

Con las anteriores definiciones podemos definir al cracker, como el especialista que logra romper la seguridad del sistema informático u operativo, cuya finalidad es denegar el acceso, destruir o robar la información contenida en la computadora, procesadores o redes.

---

<sup>49</sup> Téllez Valdés, Julio, op. cit., nota 1, p. 457.

<sup>50</sup> Azaola Calderón, Luis, op. cit., nota 48, p. 32.

Existen diferentes tipos de crackers y su nombre varía de acuerdo al fin que persigue, el especialista en Spam, se le denomina Spammer's.

- **Spammer's:**

Se contemplan a todas las personas, empresas o profesionales que se dedican al envío de correo no solicitados o "Spam".

Es denominado spammer aquel individuo o el conjunto de los mismos (incluso pueden formar una asociación y/o empresa), cuya finalidad es obtener cuentas electrónicas verdaderas (no importa donde tienen que buscar, ya que la diversidad que existe es muy amplia), al obtenerlas enviarán la mayoría de las veces publicidad muy tentativa y atractiva o peor aún, causar daño de cualquier tipo (principalmente económico), al receptor final.

El problema es que dicha población está creciendo, esto surge porque cualquier individuo que le interese puede comprar un listado enorme de direcciones 100% válidas, e iniciar su ataque a las mismas, incluso en algunos países se llega a ofrecer trabajo a las personas para realizar dichos actos desde cualquier computadora, es decir, lo consideran como un trabajo remunerado.

- **Spamming:**

Es la acción de enviar de forma masiva e indiscriminada, mensajes de carácter publicitario, se puede hacer por varias vías pero la más utilizada es el correo electrónico.

- **Individuos que intervienen en el proceso del Spam.**

- ✓ **El emisor o remitente:** es aquel individuo que redacta y envía el correo electrónico no solicitado a uno o varios destinatarios a fin de hacer de su conocimiento el contenido a los destinatarios.

- ✓ **El server emisor:** es la persona o página Web encargada de redireccionar el mail hacia la lista de los destinatarios.
- ✓ **El server receptor:** son aquellos sitios de Internet que ofrecen crear las direcciones de correo electrónico de los destinatarios, sirve de enlace, entre el server emisor y el receptor final.
- ✓ **El receptor o destinatario:** Son las personas físicas o morales, las cuales les pertenece la dirección de correo electrónico y en donde recibimos correos con contenido de Spam.

### 3.4 Características del Spam:

- a) **Anónimo:** el mayor porcentaje de los mensajes electrónicos cuyo contenido es de Spam, su verdadero origen es mediante remitentes falsos, o de contactos conocidos (pero con una dirección errónea), esto sucede porque la finalidad es hacer que el destinatario final caiga en la acción primordial que es el engaño, la trampa y así abrir dichos mensajes, por supuesto nunca sabremos quien realmente nos lo envía (en realidad si podemos), y por tanto su comprobación es imposible.
- b) **No solicitado:** muchas veces recibimos mensajes legítimos, esto es porque al formar parte o darnos de alta en algún foro, un grupo de noticias o información de nuestro interés, estaremos recibiendo información constantemente de las novedades de dichas páginas (esto sucede por aceptar su recepción), pero muchas ocasiones son enviados a la bandeja de Spam y en realidad son legítimos. Simplemente si nosotros no hemos pedido información de cualquier género, pero sobretodo de publicidad, no tenemos porque recibirla.

- c) Publicitario:** es atraer la atención del usuario final, es decir, cuando por alguna razón hemos abierto un mensaje con estas características y no lo borramos de inmediato, aplican distintas técnicas por ejemplo: ofertas insuperables de artículos de marcas prestigiosas; artículos cura-todo; viajes a precios realmente tentativos, son muchas las técnicas para engañar fácilmente (adelante veremos más información al respecto).
- d) Masivo:** esta característica es algo distintiva con estos correos electrónicos no solicitados, ya que un solo mensaje de publicidad es enviado a una cantidad enorme de emails, el fin de esta acción es que mientras más destinatarios reciban esta información, implica mayor ganancia, aunque sólo la mínima parte sean víctimas. (En adelante explicaré, como esta característica llega a repercutir en la red ocasionando serios problemas).
- e) Falta de legislación nacional e internacional vigente:** Por este motivo muchos de los ilícitos informáticos quedan impunes, al no tener una ley especializada en la materia, también quedan absueltos de pena los sujetos activos, aunque su actuar sea doloso.
- f) Fin de lucro:** la finalidad de que el Spam sea masivo, es por la sencilla razón, de que algún porcentaje de los sujetos que accedan a los medios informáticos, caigan en el engaño y así obtener ganancias, que ocasionan grandes pérdidas económicas a nivel mundial.

### **3.5 Medios Informáticos donde se presenta el Spam.**

Muchos tienen una percepción errónea en cuanto al campo de aplicación del Spam, si bien es cierto que en el lugar en donde se presenta con un mayor porcentaje es a través del correo electrónico; pero esta no es la única manera en la cual se puede presentar, existen diversos y nuevos métodos los cuales

desconocemos. Abordaré dicha problemática para conocer los métodos utilizados y sobretodo defendernos tomando las medidas adecuadas.

- Correo electrónico: El email o correo electrónico es una herramienta que vino a revolucionar la comunicación a distancia, ya que podemos hacerlo en un instante; encontrándose tanto el destinatario, como el remitente, en cualquier parte del mundo.

Lamentablemente es muy vulnerable con respecto al Spam, aunque existen filtros anti-Spam estos no son muy seguros ya que nos siguen llegando este tipo de correos.

Algo que muy pocas personas saben, es que se encuentra en peligro de extinción, es decir, puede desaparecer de un momento a otro, esta acción tan radical la verdad no resuelve nada, se tiene que concientizar a todos los que usamos esta herramienta para poder atender el problema de raíz; sancionar a los culpables; que todas aquellas personas que no solo han sido agredidas en su patrimonio sino también en su integridad, no queden impunes dichos actos, que los han convertido en víctimas, como consecuencia del Spam.

- Mensajería instantánea *spim* (simulador que ejecuta programas): Como podemos darnos cuenta, poco a poco tenemos algo de conocimiento sobre la constante aparición del tema, los individuos responsables están buscando nuevas formas para atacarnos.
- Foros: Esta clase de Spam, es realmente muy extraña ya que la mayoría prefiere mantener el anonimato, pero aquí generalmente los mismos usuarios hacen una constante referencia, sobre algún enlace que por lo general no tiene relevancia con el tema en comento.

Preocupa mucho a los creadores de los distintos foros, ya que dichos enlaces o links, generan a su vez otros enlaces, los cuales nos dirigen a diversos temas de interés, cuyo resultado es que en el foro principal hay menos usuarios, es decir, los comentarios en el primer foro han sido desplazados al acceder a otra circunstancia.

- Blogs: Básicamente abarca todo lo relevante en cuanto a debates, discusiones mismas que son abiertas para todos aquellos a quienes les interese, su finalidad es hablar al respecto y compartir nuestras opiniones en una temática de cualquier índole e interés.

El problema es cuando algún usuario hace referencia de una manera persistente sobre publicidad de cualquier tipo, ya sea algún sitio web, mercancía, etc. Es decir, al insistir de tal forma, nos da la certeza que nos estamos enfrentando a un tipo de Spam, hay determinadas reglas para contrarrestarlo por ejemplo: se puede excluir al usuario de forma temporal y/o permanente; incluso cerrar el blog para no seguir acumulando Spam.

- Teléfonos móviles: Esta modalidad es la que estamos sufriendo actualmente, es a través de servicios de mensajería instantánea (SMS), la verdad es muy molesto estar recibiendo estos mensajes, ya que la mayoría de las veces la información y/o publicidad, simplemente no son de nuestro interés.

Hay que resaltar que estos mensajes son enviados a nuestros celulares, por nuestra compañía telefónica, para hacernos saber alguna novedad en su servicio, aquí es donde se aprovechan los spammer's al saber que los destinatarios podrán ser engañados, ya que nosotros al ver el nombre o las siglas de nuestra compañía telefónica damos por hecho que es auténtico.

Un ejemplo de esto es: Si nosotros abonamos \$100.00 pesos enviando la respuesta a determinado mensaje obtendremos \$300.00 pesos en tiempo aire, a simple vista parece ser una buena oferta, pero al observar muy

cuidadosamente en la serie de dígitos, sabremos que un par de números pueden cambiar todo y nos quedaremos sin nada. Ya que estaremos enviándole al spammer saldo gratis, es decir, de nuestro bolsillo.

- Grupos de noticias: Esta herramienta es utilizada por algunos usuarios en la red, para poder opinar sobre un tema en común con algunas otras personas, que pueden ser miembros de dicho servicio y por lo tanto dar su punto de vista en el mismo, hay que mencionar que la mayoría de las veces es de carácter público y cualquiera puede comentar ya sea a favor o en contra, también existen grupos privados para empresas, estos son más serios en cuanto a la dinámica.

Lamentablemente se están utilizando técnicas sin ningún escrúpulo, se menciona cualquier noticia que pasa en el mundo, mientras más fuerte sea, los receptores finales accederán al ser impactados por lo acontecido.

Verbigracia: “Lo acontecido con el temblor de Haití, cuyo país fue devastado casi en su totalidad;” entonces es cuando se empieza el ataque masivo e indiscriminado en correo o mail, y básicamente diría “si quieres brindar tu apoyo puedes hacerlo al número de cuenta determinado” el cual pertenece a otra persona y no a la fundación mencionada.

### **3.6 Temas del Spam.**

Naturalmente los temas serán aquellos relacionados con artículos novedosos, de marcas reconocidas mundialmente, pero con un atractivo descuento que es difícil no querer, lo interesante es que dicho mensaje de publicidad cumple su primer objetivo, el cual es dar click sobre éste para acceder al link que muchas de las veces aparenta ser un sitio oficial, para que el usuario no desconfíe en ningún momento y otorguemos información confidencial sobre

nuestras cuentas bancarias, datos personales; sin darnos cuenta de los motivos que estimen al tenerlos en su poder.

- Pornografía:

Este tipo de publicidad es la de mayor abundancia en Internet, cuyo contenido es solo para mayores de edad, puede contener texto explícito en cuanto al tema e incluso imágenes ofensivas o incómodas, ya que al presionar dicho anuncio nos dirige a un sitio web el cual no era el tema que se presentó y nos lleva a sitios sexuales o eróticos que por más que cerremos esa ventana se abrirán otras. Incluso cuando iniciamos cesión para navegar en Internet aparecen imágenes de dicha índole, acompañadas con la página de inicio. Para deshacernos de esta molestia lamentablemente se tiene que volver a instalar el navegador de Internet de nuestra preferencia.

- Salud:

En esta modalidad a muchos de verdad nos llegaría a interesar la información que estamos recibiendo, esto es porque en algún momento nosotros o algún familiar cercano, tiene un problema de salud y curiosamente el producto que nos muestran lo puede solucionar, en la realidad estos productos son mejor conocidos como “cura todo” y en verdad no curan nada. También podemos encontrar ofertas de medicamentos que nos interesaría comprar, lamentablemente es apócrifa dicha información.

- Piratería:

A decir verdad este es el tema más utilizado tanto en la red, como en los demás medios donde se llega a propagar dicho fenómeno, por ende seremos atacados a través de publicidad de una amplia gama de artículos de cualquier índole por el fenómeno del Spam, ya que no solo abarca discos, películas también medicamentos, ropa, es decir todo aquello que pertenece a una marca mundialmente reconocida, misma que podemos adquirir a un precio muy accesible y en alguna ocasión podemos caer en la trampa.

- Educación:

Si bien sabemos somos atacados por diferentes métodos y campos de aplicación en cuanto al correo no solicitado, la finalidad de estos individuos no tiene límites. Buscan persuadir con ofertas en el ámbito de la educación, básicamente para diplomados, maestrías, seminarios, etc., todo esto es a través de cursos en línea, pero antes de acceder hay que informarnos sobre la veracidad de todo esto para no ser víctima o acreedor a una sanción por dichos actos.

### 3.7 Definiciones a fines.

**a) Definiciones de acuerdo a las modalidades del Spam:** Pero por si fuera poco el Spam no viene solo, ya que incluyendo a los spammer's, aparecen otras figuras las cuales muchos desconocen su existencia y sobre todo los daños que generan; abordare estas mismas para conocer los efectos que producen.

- Scam:

- ✓ “Fraude destinado a conseguir que una persona o grupo de personas entreguen dinero, bajo falsas promesas de beneficios económicos (viajes, vacaciones, premios de lotería, etc.).”<sup>51</sup>
- ✓ “Es el delito consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro; utilizando como medio la tecnología.”<sup>52</sup>
- ✓ “Es utilizado para referirse a correos relacionados con publicidad engañosa.”<sup>53</sup>

---

<sup>51</sup> Interbusca. Disponible en: <http://antivirus.interbusca.com/glosario/SCAM.html>, consultada el 29 de febrero de 2012 a las 18:30 horas.

<sup>52</sup> Eset. Disponible en: <http://www.eset-la.com/centro-amenazas/amenazas/2146-Scam>, consultada el 01 de marzo 2012 a las 10:00 horas.

Desde mi punto de vista podemos encasillar a este tipo de correos electrónicos en un solo concepto, el cual trata de enviar al receptor final una serie de oportunidades para ganar algo de dinero, sin perder nada a cambio, obvio aunque esta idea es muy buena, la realidad no es así, porque se trata de una estafa, pero no sólo abarca los correos electrónicos que se reciben, sino también sobre las páginas o sitios en Internet que hacen mal uso de la información, todo esto sucede al recibir información que es totalmente falsa.

- **Spim**: Este tipo de figura surge como una variable del Spam, se basa en los efectos del problema principal, pero la diferencia en su modo de actuar es a través de la mensajería instantánea o chats (*MSN de Microsoft, Yahoo! Messenger o AOL Messenger*, entre otros).

En esta modalidad es muy probable que demos un clic a un mensaje o link determinado sin pensarlo bien, esto es porque mientras nos encontramos en una conversación y éste actúa como un molesto distractor por lo que, accedemos a él, con tal de desaparecerlo instantáneamente y poder continuar nuestra plática y desfavorablemente caemos en la trampa.

- **Spit** (Spam sobre telefonía IP): La telefonía IP consiste en la utilización de Internet como medio de transmisión para realizar llamadas telefónicas.
- **Vishing** (Fraude que persigue el mismo fin que el *Phishing*): La obtención de datos confidenciales de usuarios, pero a través de un medio distinto: como la telefonía IP. Los ataques de vishing se suelen producir siguiendo dos esquemas:

---

<sup>53</sup> Castellanos Hernández, Eduardo, *et al.*, *Temas de Derecho Informático*, México, Orden jurídico nacional, Secretaría de Gobernación, SEGOB, 2006, p.p. 152, 153.

- ✓ Envío de correos electrónicos, en los que se alerta a los usuarios sobre algún tema relacionado con sus cuentas bancarias, con el fin de que éstos llamen al número de teléfono gratuito que se les facilita.
- ✓ Utilización de un programa que realice llamadas automáticas a números de teléfono de una zona determinada.

En ambos casos, cuando se logra contactar telefónicamente con el usuario, un mensaje automático le solicita el número de cuenta, contraseña, código de seguridad, etc.

- ***Phishing***: Fraude tradicionalmente cometido a través de Internet, que pretende conseguir datos confidenciales de usuarios como contraseñas o claves de acceso a cuentas bancarias. Para lograr esta información, se realizan envíos masivos de correos electrónicos, que simulan proceder de entidades de confianza. En el mensaje se pide al usuario que, por "motivos de seguridad" o con el fin de "confirmar su cuenta", facilite sus datos personales, claves, etc. En ocasiones, este tipo de datos se solicitan en el mismo mensaje, o se indica al usuario que acceda a la página web de la entidad en cuestión, que es una copia idéntica de la original, donde deberá completar dicha información. Actualmente están surgiendo numerosas versiones de este delito, que se sirven de otro tipo de medios para conseguir los mismos fines. Un ejemplo del nuevo *phishing* es el *Smishing*.

#### **b) Delitos relacionados con el Spam:<sup>54</sup>**

- **Intrusismo informático o *hacking* informático**: "...la mera entrada o acceso a sistemas informáticos por el simple gusto de superar las medidas de seguridad de los sistemas informáticos, sin intención o sin la

---

<sup>54</sup> Azaola Calderón, Luis, op. cit., nota 48, p.p. 61-73.

finalidad de manipular, defraudar, cometer sabotaje o espionaje informático.”

- **Espionaje informático:** Para Rovira de Canto es “el conjunto de actividades de obtención no autorizada de datos o información de carácter sensible, esto es, confidenciales o secretos, de contenido y valor económico patrimonial, y/o divulgación no autorizada de los objetos legítimamente, con ánimo de lucro y en perjuicio de tercero.”
  
- **Sabotaje informático:** “... consiste, básicamente, en borrar, suprimir o modificar sin autorización o datos de las computadoras con intención de obstaculizar el funcionamiento normal del sistema. La técnica más conocida para cometer este tipo de actividad es la que conocemos comúnmente con el nombre de <<virus informático>>.”
  
- **Virus informático:**
  - ✓ “...es un programa que puede ingresar en un sistema a través de cualquiera de los métodos de acceso de información externa. Se instala, se reproduce y causa diversos daños.”
    - a) Gusanos: Se infiltran en los programas ya sea para modificar o destruir los datos, pero se diferencian de los virus porque estos no pueden regenerarse.
  
    - b) Bomba lógica: es la introducción en un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha o circunstancia, destruyendo datos de la computadora, distorsionando el funcionamiento del sistema o paralizando el mismo.
  
  - ✓ Una aportación de Pablo Andrés Palazzi sobre esta misma tesitura nos menciona lo siguiente: “para poder abarcar todo el sentido de

lucha con el problema de los virus se requiere la modificación de artículos existentes, ligados al delito de daño pero con aspectos que propicien lo preventivo. La redacción debería tener como estructura básica el tipificar como ilícito la producción y distribución de virus informáticos.”<sup>55</sup>

- **Distribución de Virus:** “Es la acción de enviar el virus a un equipo ajeno. Es el que mayores complicaciones puede tener, ya que el agente puede enviar a un tercero el archivo infectado sin darse cuenta o bien sin haber realizado los controles necesarios.”<sup>56</sup>
- **Fraude informático:** “...consiste en cualquier conducta y/o manipulación realizada a través o por medio de un sistema informático, con el objeto de obtener un beneficio ilegítimo, ocasionando un perjuicio a una o varias personas.”<sup>57</sup>

Para Moránt Vidal J. existen supuestos de conductas de fraude informático:

- a) **Daños engañosos:** se traduce en manipulaciones del ordenador, tendientes a introducir informaciones falsas, o a eliminar aquellas que son verdaderas.
- b) **Caballo de Troya:** implica la introducción de un conjunto de instrucciones para que el ordenador lleve a cabo operaciones no autorizadas.<sup>58</sup>
- c) **La técnica del Salami:** que permite sustraer mediante redondeo pequeñas cantidades de activos financieros de diversas cuentas

---

<sup>55</sup> Palazzi, Pablo Andrés, *Delitos informáticos*, Buenos Aires, Argentina, Ad-Hoc, 2000, p. 160.

<sup>56</sup> Cámpoli, Gabriel Andrés, op. cit., nota 45, p. 20.

<sup>57</sup> Azaola Calderón, Luis, op. cit., nota 48, p.p. 72-73.

<sup>58</sup> Aunque en esta clasificación se encuentra dentro del fraude informático, es considerado también como un virus, conocido comúnmente como troyano.

bancarias para situar su monto total, que puede ascender a cantidades considerables de la cuenta del delincuente.”<sup>59</sup>

### **3.8 Daños que ocasiona el Spam.**

Aunque suene imposible que un solo acto (por lo general es un correo electrónico), genere una serie de acontecimientos en cadena en cuanto a los efectos ocasionados; pero este mismo puede llegar a repercutir en una persona o hasta un desastre de una nación (misma que no ha tomado cartas en el asunto, creando una ley para contrarrestar dicho problema), el obstáculo que se tiene es el gran desconocimiento del tema; por lo tanto se le resta la importancia que en realidad debería de tener, si bien es cierto que actualmente se escucha hablar un poco más al respecto, la verdad es que no se conocen los grandes efectos ocasionados por el Spam (correo electrónico de publicidad no solicitado). Hablaremos sobre las consecuencias de este problema para adentrarnos y tener nuestra mejor opinión al respecto.

Son varios los efectos producidos por culpa del Spam, llega a ocasionar el llamado “tráfico de correo electrónico” en la red, esto es porque se envían y reciben más correos de esta índole, a comparación con los mails que en verdad son legítimos, a decir verdad esta última cantidad es mínima, causando una saturación en el servicio.

En muchas ocasiones esperamos un mail importante, y simplemente no nos llega a tiempo y/o si hemos recibido el correo, pero no aparece en la bandeja de entrada porque se encuentra en una carpeta que usualmente no vemos.

---

<sup>59</sup> Azaola Calderón, Luis, op. cit., nota 48, p.p. 69-70.

Mostrare unos datos obtenidos para ver la totalidad de correos electrónicos, que circulan en la red, cuántos de ellos son limpios y cuantos contienen Spam como veremos en las siguientes cifras:

	<b>MÉXICO (2010).</b>
Enviados.	5, 757, 353.
Enviados <b>eliminados</b> SPAM.	4, 888, 072.
Enviados <b>limpios</b> .	<b>869, 271.</b>

	<b>MUNDO (2010).</b>
Recibidos del Mundo.	93, 181, 485.
Recibidos <b>eliminados</b> SPAM.	91, 101, 195.
Recibidos <b>limpios</b> (Promedios diarios).	<b>2, 080, 291.</b>

Es notable la gran diferencia que existe, esto es debido a que no se aprovecha adecuadamente dicha herramienta, la cual es de mucha utilidad en nuestras actividades, en cuanto a la comunicación a distancia.

También se produce una pérdida de tiempo (la cual es muy tediosa), pero sobre todo una gran pérdida monetaria; este punto es importante resaltarlo ya que el tiempo que es utilizado en revisar cada correo electrónico en la carpeta de Spam y estar borrando uno por uno, (aunque sería más fácil borrar toda la carpeta), aunque esto sería un error para nosotros, porque muchas veces hay emails válidos que nos envían y se guardan en dicha carpeta (por error), entonces si realizamos la acción anteriormente mencionada perderemos información que es realmente válida.

Resulta difícil creer que el tiempo estimado en hacer dicha actividad no cause daño alguno, la verdad es que representa grandes pérdidas monetarias,

sobretudo aspectos en cuanto a la efectividad laboral, ya que este tiempo sería mejor aprovechado para mejorar el trabajo.

Los que más sufren este tipo de problemas son aquellos que tienen una cuenta privada de correo electrónico, así como las cuentas de empresas, consorcios, etc., muy reconocidos en sus campos de trabajo y por ende reciben diariamente una cantidad enorme, por lo tanto mientras más Spam exista, mayor será el tiempo dedicado a resolverlo (hay que mencionar que si no lo hacemos en ese momento, tal vez cuando accedamos otra vez estará saturada y no podremos recibir uno nuevo).

Otro problema es que pueden confundirnos como un spammer, esto puede suceder porque usan nuestro equipo como una computadora “*zombi*”, (esto pasa por que nuestra Dirección IP es utilizada para enviar Spam) y seremos los responsables de practicar dicha actividad a una lista interminable denominada “lista negra”, causando demasiados estragos.

También está muy latente la probabilidad de ser atacados por un virus el cual puede borrar toda nuestra información, como se ha visto también se ve afectado el Internet, en cuanto al servicio de ancho de banda por no utilizarse correctamente. Pueden usar nuestro equipo de cómputo no sólo para que nosotros seamos los remitentes de dichos actos, también para seguir buscando en la red más direcciones válidas usándonos como “*carnada*” y no darnos cuenta de todas estas acciones.

No todos los daños son materiales existe información sobre personas que han sido amenazadas y/o golpeadas si no ofrecen datos confidenciales, contraseñas de sus cuentas bancarias, etc.; lamentablemente se conocen datos sobre personas que han sido asesinadas por no acceder a las peticiones de los spammer's.

Por todo lo mencionado con anterioridad vemos que el Spam no es sólo una serie de actos, cuya finalidad es obtener dinero sin esforzarse tanto, va más allá de nuestras expectativas y si se conociera a fondo el problema pero sobretodo se sancionara a los responsables, no se seguirían cometiendo más delitos impunemente.

### **3.9 Tipos de Spam más comunes en México.**

En nuestro país se creería que no sufrimos las consecuencias del correo electrónico comercial no solicitado, pero actualmente estamos siendo invadidos por las trampas que día a día son más novedosas.

Los spammer's se aprovechan en diversos campos donde podemos ser muy vulnerables, varias veces por la situación que se encuentra el país, ya sea por alguna catástrofe, algún evento importante que nos atañe a todos y/o por restarle importancia al ser descuidados y no observar la veracidad del engaño; por ejemplo, una página web de un banco que al parecer es auténtica, pero si vemos detenidamente descubriremos la farsa; otro seria algún desafortunado evento natural, mismo que impacto a todo el mundo y queremos ayudar, entonces los spammer's aprovechándose de la situación empiezan a mandar correos maliciosos, diciendo que si queremos ayudar podemos hacerlo a través de determinado sitio, el cual al acceder podría parecer autentico, pero la verdad no es así.

- Cadenas: este tipo de correos son los que más saturan nuestros correos y aunque los borramos siguen llegando, cuando entramos a nuestro mail, vemos que hay cientos de mensajes que forzosamente abriremos uno a uno, ya que al estar mezclados con correos limpios no podemos borrarlos todos; lo que en verdad no comprendo es como la gente las sigue reenviando.

- Trabajos falsos: aquí simplemente se trata de personas que nos contactan, sabiendo que hemos solicitado determinado puesto y aseguran asignárnoslo si damos un dinero a cambio, otra trampa es un negocio fácil con grandes ganancias, haciéndonos saber estrategias tentadoras que simplemente son mentiras.
- Saldo gratis para celular: El mensaje es que si nosotros ingresamos crédito a nuestro celular nos regalan incluso más del doble de saldo. En esta nueva manera de recibir Spam la verdad es muy difícil no caer, ya que no debe existir un mínimo margen de error con la finalidad de que el receptor caiga en la trampa, en verdad hay que ser perspicaces en ese sentido porque aunque el mensaje o la publicidad parezca oficial y/o verdadera todo puede ser falso cambiando solamente una letra incluso un número.

Aunque resulte ilógico que alguien no alcancé a percibir que todo se trata de una farsa, cuyo objetivo es enviarle a otra persona nuestro dinero por medio de una transacción electrónica a cambio de nada, muchos instantáneamente diríamos que por supuesto es un mínimo porcentaje, pero la realidad es otra ya que se tiene estimado a nivel mundial, millones de dólares en pérdidas de índole general a consecuencia del Spam, en otras palabras existen muchos que creen en este tipo de publicidad considerándola confiable y autentica.

Actualmente nos encontramos en una situación muy peculiar en cuanto al tema, me refiero a que todos creemos que el emisor de Spam número uno en el mundo es Estados Unidos (su posición es muy variable), pero hablando en forma general, es decir, de continentes resulta difícil creer que el continente Asiático va a la cabeza (gracias a países como Vietnam, Corea que al parecer esta haciendo todo para ocupar el primer puesto y desplazar a E.U., China, Rusia).

En especial India es el principal emisor de correos electrónicos no solicitados en el mundo, los países que lo siguen son Italia y posteriormente

Arabia Saudita, se tienen datos de que su población en utilizar Internet sólo representa el 5%, a comparación los grandes potencias como Estados Unidos de América y China que representan el 10%.

Pero increíblemente le sigue toda América Latina (este fenómeno se debe a que países como Argentina, Brasil sobre todo este último están practicando dicha actividad ilícita de una manera constante); se encuentra muy cerca Europa Occidental, es importante señalar que va ganando terreno en contra de dicha problemática, por fin aparece Norteamérica (especialmente los Estados Unidos como todos sabemos genera a gran escala Spam, pero el último trimestre del 2010 pudo desaparecer del top 20 es algo inaudito y hay que admirarlo).

Después nos encontramos con Europa Oriental (aunque España logro salir del listado a nivel mundial de Spam, hace lo imposible por volver a entrar) y por último tenemos al continente Australiano (de alguna manera está logrando erradicar dichos correos electrónicos aunque sigue teniendo un mínimo porcentaje) y Africano (por obvias razones tiene un porcentaje casi nulo).

Para observar de una mejor manera mostrare una tabla, para entender de una manera más grafica dicha información obtenida de la siguiente página en Internet.<sup>60</sup>

<b>PAÍSES.</b>	<b>% DE SPAM (2012).</b>
INDIA	16.1
ITALIA	9.4
ESTADOS UNIDOS	6.5
ARABIA SAUDITA	5.1
BRASIL	4.0
TURQUÍA	3.8

<sup>60</sup> Disponible en: <http://nakedsecurity.sophos.com/2012/10/16/india-spews-more-spam-than-ever-before-report-finds/>, consultada el 01 de junio de 2012 a las 14:00 horas.

<b>PAÍSES.</b>	<b>% DE SPAM (2012).</b>
FRANCIA	3.7
COREA DEL SUR	3.6
VIETNAM	3.4
CHINA	3.1
ALEMANIA	2.7
REINO UNIDO	2.1
OTROS	36.5

Como podemos observar este no sólo es un problema de un país o un continente, sino que nos perjudica a todos ya que al tener una dirección electrónica con cualquier servidor del mismo, formamos parte de un ciclo que con la ayuda de todos podemos frenar estas acciones maliciosas de los spammer's.

Pero sólo podremos aportar nuestra ayuda con la creación de una ley muy clara y consistente, para apoyar a todas aquellas personas que han sido víctimas, saber que pueden denunciar dichos actos, que nuestras autoridades y sobretodo los jueces cuenten con la herramienta adecuada para aplicar sanciones a todos aquellos que están cometiendo actos ilícitos.

Lamentablemente el correo electrónico comercial no solicitado no sólo implica una gran molestia en nuestras bandejas de entrada de nuestros e-mails, sino que va más allá, porque no son las mismas pérdidas tanto económicas como en cuestión de tiempo, esto se debe a que las personas que poseen correos electrónicos de un servidor de paga (como una empresa) reciben una cantidad mayor diariamente a comparación de nosotros que sólo recibimos algunos cuantos.

La verdadera razón por la que surge la problemática en cuestión, se debe a la falta de seguridad informática que tenemos culturalmente.

**CAPÍTULO IV**  
**ANÁLISIS DOGMÁTICO DEL SPAM.**  
**Aspectos positivos y Negativos del delito.**

*“Si esto es así, entonces debemos concluir que desde el punto de vista, los elementos del delito en materia penal, federal coinciden con la estructura del delito en sus diversas etapas (causalismo clásico, neoclásico, etc.). las principales diferencias radican en las cuestiones filosóficas y metodológicas, el lugar que ocupa cada una de ellas, además de su contenido.”<sup>61</sup>*

**BIEN JURÍDICO TUTELADO.**

Antes de entrar en materia de estudio del ilícito penal, es necesario dejar claro la definición del bien jurídico tutelado:

“Es un valor ideal del orden social no perceptible a través de los sentidos sino deducible intelectualmente.”<sup>62</sup> “tiene un carácter abstracto, es decir, su valor se incorpora no sólo en objetos materiales, sino también puede consistir en un valor o cualidad sumamente valiosa para la sociedad.”<sup>63</sup>

Ejemplo de ello es la afectación que sufrimos en nuestra persona, es decir, en nuestro patrimonio, seguridad de la información, etc.

Para que un hecho sea sancionado debe causar un daño en la esfera jurídica del gobernado, y por lo tanto, este mismo tiene que estar plasmado en las leyes penales. El estudio de estas conductas ilícitas lo realiza el derecho penal, mediante la dogmática jurídica. De aquí se desprenden diversas teorías,

---

<sup>61</sup> Jiménez Martínez, Javier, *Elementos de Derecho Penal Mexicano*, México, Porrúa, 2006, p. 288.

<sup>62</sup> Urosa Ramírez, Gerardo Armando, *Teoría de la Ley Penal y del delito*, México, Porrúa, 2006, p. 109.

<sup>63</sup> Díaz Aranda, Enrique, *Derecho penal. Parte general*, 3ª. ed., México, Porrúa, 2003, p. 79.

las cuales contemplan desde 2 hasta 7 aspectos positivos y negativos del delito, según sea el sistema penal de cada país.

De acuerdo con la doctrina en base a la Teoría Analítica o Atomizadora, se estudiará al delito en sus aspectos positivos y negativos, como se puede ver en el cuadro proporcionado por Jiménez de Asúa.

<b>ASPECTOS POSITIVOS</b>	<b>ASPECTOS NEGATIVOS</b>
ACTIVIDAD	FALTA DE ACCIÓN
TIPICIDAD	AUSENCIA DE TIPO
ANTI JURIDICIDAD	CAUSAS DE JUSTIFICACIÓN
IMPUTABILIDAD	CAUSAS DE INIMPUTABILIDAD
CULPABILIDAD	CAUSAS DE INCULPABILIDAD
CONDICIONES OBJETIVAS	FALTA DE CONDICIÓN OBJETIVA
PUNIBILIDAD	EXCUSAS ABSOLUTORIAS

#### **4.1 Conducta.**

El primer concepto de conducta se puede comprender del contenido establecido en el Artículo 7 del Código Penal Federal.

“Delito es el acto u omisión que sancionan las leyes penales.”<sup>64</sup>

De conformidad con la teoría heptatómica y el anterior cuadro, el primer elemento del delito es la conducta, la cual considero como aquella manifestación de la voluntad, va encaminada, a la realización de un resultado. En la doctrina es adecuado hablar de conducta porque en ella se encuadra al acto y omisión. Aduciendo a lo anterior es pertinente definir primeramente a la conducta.

---

<sup>64</sup> Código Penal Federal, nota 25.

El Poder Judicial de la Federación menciona que la conducta:

1. “Puede expresarse en forma de acción (actividad voluntaria o involuntaria) y de omisión, comprendiendo está última la omisión simple y la comisión por omisión.”<sup>65</sup>
2. Para Fernando Castellanos Tena, la conducta es: “El comportamiento humano voluntario, positivo o negativo, encaminado a un propósito.”<sup>66</sup>
3. Para Carranca y Rivas, Raúl, considera a la conducta como: “El acto consiste en una acción positiva, en un hacer, lo que no se debe hacer, en un comportamiento que viola una norma que prohíbe; la omisión en una actividad negativa, en un dejar de hacer lo que se debe hacer, en un omitir obediencia a una norma que impone un deber de hacer. Ambos son conducta humana, manifestación de voluntad que produce un cambio o peligro de cambio en el mundo exterior, llamado resultado.”<sup>67</sup> Del anterior concepto se desprenden los siguientes elementos:

**b) Acción:**

Básicamente es la manifestación del actuar humano para poder hacer o realizar, determinada actividad, misma que puede llegar a infringir una norma jurídica y ser acreedor a una pena. Eugenio Cuello Calón, define a la acción como “el movimiento corporal voluntario encaminado a la producción de un resultado consistente en la modificación del mundo exterior o en el peligro de que se produzca.”<sup>68</sup> Para el alemán Claus Roxin, explica “el concepto de acción como manifestación de la personalidad es idóneo como elemento básico, al abarcar todas las formas de manifestación de la conducta delictiva y, aparte de ello, todo lo que en el campo prejurídico tiene sentido calificar como acciones.”<sup>69</sup> Se entiende

---

<sup>65</sup> Aguilar López, Miguel Ángel, *El delito y la responsabilidad penal*. Teoría, jurisprudencia y práctica, 4ª. Ed., México, Porrúa, 2008, p. 335.

<sup>66</sup> Castellanos Tena, Fernando, *Lineamientos elementales de Derecho penal. Parte general*, 44ª. ed., México, Porrúa, 2003, p. 149.

<sup>67</sup> Aguilar López, Miguel Ángel, op. cit., nota 65, p. 29.

<sup>68</sup> *Ibidem*, p. 152.

<sup>69</sup> Jiménez Martínez, Javier, *Introducción a la teoría general del delito*, 2ª. ed., México, Ángel Editor, 2005, p. 424.

que los principales elementos de la acción es el hacer y el querer, tal como lo explica Edmundo Mezger: “En la acción se encuentran los siguientes elementos: un querer del agente, un hacer del agente y una relación de causalidad entre el querer y el hacer.”<sup>70</sup>

El Correo Electrónico no Solicitado es una conducta únicamente de acción como se desprende de los artículos 17, 18, 18 BIS, 32 de la Ley Federal de Protección al Consumidor, cuando se refiere al verbo rector enviar o utilizar información con fines diferentes a los mercadotécnicos o publicitarios, ceder, transmitir, inducir, al consumidor al error con engaños abusivos.

### **Ley Federal de Protección al Consumidor.**<sup>71</sup>

*“**Artículo 17.-** en la publicidad que se **envíe** a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, **envíe** la publicidad a nombre del proveedor, y de la procuraduría.*

*El consumidor podrá exigir directamente a proveedores específicos y a empresas que **utilicen** información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le **envíen** publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que **utilicen** información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea **cedida** o **transmitida** a terceros, salvo que dicha **cesión** o **transmisión** sea determinada por una autoridad judicial.”*

---

<sup>70</sup> Castellanos Tena, Fernando, nota 66, p. 156.

<sup>71</sup> Ley Federal de Protección al Consumidor, nota 27.

**“Artículo 18.-** la procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea **utilizada** para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo electrónico a la procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito.”

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

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

*Para los efectos de esta ley, se entiende por información o publicidad engañosa o abusiva aquella que refiere características o información relacionadas*

*Con algún bien, producto o servicio que pudiendo o no ser verdaderas, **inducen** a error o confusión al consumidor por la forma inexacta, falsa, exagerada, parcial, artificiosa o tendenciosa en que se presenta.*

*La información o publicidad que compare productos o servicios, sean de una misma marca o de distinta, no podrá ser engañosa o abusiva en términos de lo dispuesto en el párrafo anterior.*

*La procuraduría podrá emitir lineamientos para el análisis y verificación de dicha información o publicidad a fin de evitar que se **induzca** a error o confusión al consumidor, considerando el contexto temporal en que se difunde, el momento en que se transmite respecto de otros contenidos difundidos en el mismo medio y las circunstancias económicas o especiales del mercado.”*

### **c) Omisión.**

El hablar de omisión es referirnos al dejar de hacer, lo previsto en la norma, tal como nos indica Eugenio Cuello Calón, la omisión: “Consiste en una inactividad voluntaria cuando la Ley penal impone el deber de ejecutar un hecho determinado.”<sup>72</sup> Para Griselda Amuchategui Requena, “consiste en realizar la conducta típica con abstención de actuar, esto es, no hacer o dejar de hacer.”<sup>73</sup>

La omisión se subdivide en:

- 1. Omisión Simple o propia:** Fernando Castellanos Tena afirma que la omisión simple “consiste en un no hacer, voluntario o culposo, violando una norma preceptiva, produciendo un resultado típico.”<sup>74</sup> Arturo Jiménez Zamora considera que: “se castiga el no hacer de la acción esperada y exigida como tal, no siendo necesario un resultado.”<sup>75</sup>
- 2. Omisión impropia o de comisión:** Para Celestino Porte Petit “existe un delito de comisión por omisión, cuando se produce un resultado típico y

---

<sup>72</sup> Castellanos Tena, Fernando, op. cit., nota 66, p. 153.

<sup>73</sup> Amuchategui Requena, Griselda, *Derecho Penal*, 3ª. ed., México, Oxford, 2005, p. 55.

<sup>74</sup> Castellanos Tena, Fernando, op. cit., nota 66, p. 154.

<sup>75</sup> Jiménez Zamora, Arturo, *Manual de Derecho Penal*, México, Ángel Editor, 2000, p. 118.

material, por un no hacer, voluntario o culposo (delitos de olvido) violando una norma preceptiva (penal o de otra rama del Derecho) y una norma prohibitiva.

Elementos:

- Voluntad,
- Inactividad,
- Resultado material (típico),
- Relación de causalidad entre dicho resultado y la abstención.”<sup>76</sup>

Se concluye que en el correo electrónico no solicitado establecido en la Ley Federal de Protección al Consumidor se excluye a la omisión por ser una conducta de acción.

- **AUSENCIA DE CONDUCTA.**

Considerada como el aspecto negativo de la culpabilidad, se desprende del **Artículo 15** fracción primera del Código Penal Federal.

“El delito se excluye cuando:

- I. El hecho se realice sin intervención de la voluntad del agente”<sup>77</sup>

Como causa o supuestos de ausencia de acción, la doctrina suele analizar aquellos actos del hombre que no reúnen los caracteres de voluntad final, distinguiendo tres supuestos:

**A) Fuerza Física Irresistible.**

- Vis Absoluta:

---

<sup>76</sup> Ídem.

<sup>77</sup> Código Penal Federal, nota 25.

En este tipo de ausencia existe una fuerza irresistible, misma que negará al individuo evitar dicha conducta.

- Vis Maior o fuerza mayor:  
Surge cuando el individuo es impedido a través de una fuerza de la naturaleza o subhumana.

## **B) Los movimientos reflejos.**

Son contrarios a la voluntad del individuo, ya que estos se generan involuntariamente respondiendo a una acción.

## **C) Estado de inconsciencia y las acciones libres en su causa.**

- El sueño profundo,
- Sonambulismo,
- Embriaguez, e
- Hipnotismo.

Es necesario aclarar que estos estados se pueden o no generar, pero sin la voluntad del hombre.

Dichas características de la ausencia de conducta, en este precepto no se presentan, ya que tanto la vis absoluta, como la vis mayor no tienen lugar; porque se necesita repeler una fuerza física irresistible, pero sobre todo una computadora para cometer sus ilícitos a través del Spam, y de la cual no es un ser humano. Tampoco se presentan los movimientos reflejos ni el estado de inconsciencia, se necesita de la plena capacidad del sujeto activo de conocer y comprender, por tanto contar con la capacidad de entender su actuar.

## 4.2 Tipicidad.

Es el siguiente elemento positivo a constatar para la existencia del ilícito, en él se deben acreditar todos los elementos descriptivos del tipo. La tipicidad según la Suprema Corte de Justicia de la Nación señala, “para que una conducta humana sea punible conforme al derecho positivo, es preciso que la actividad desplegada por el sujeto activo se subsuma al tipo legal.”<sup>78</sup> Para Carlos Daza Gómez es “El elemento tipicidad es la descripción externa de la acción sin contenido normativo ni elementos subjetivos. Su relación con la antijuridicidad hace fijo como indicio. La tipicidad resulta una característica objetiva sin valoración o subjetividad (incolora o sin sangre). Lo que interesa constatar es el resultado producido por la acción y la relación de causalidad. La tipicidad es descriptiva y objetiva.”<sup>79</sup>

Tal como se establece en el **artículo 14** Constitucional 2° párrafo.  
“A ninguna ley se dará efecto retroactivo en perjuicio de persona alguna. En los juicios del orden criminal queda prohibido imponer, por simple analogía y aun por mayoría de razón, pena alguna que no esté decretada por una ley exactamente aplicable al delito que se trata.”<sup>80</sup>

A continuación estableceré las diferencias entre Tipo; Tipicidad; Juicio de Tipicidad.

El **Tipo**, es la descripción que se hace en la ley penal de la conducta de acción u omisión, que violenta el bien jurídico protegido, mientras que la **Tipicidad** es la adecuación de la conducta con el tipo penal establecido en la ley, esto se logra gracias a el silogismo lógico-jurídico que realiza el juzgador para

---

<sup>78</sup> (Semanario Judicial de la Federación, CXVII. Pág. 731). “La atipicidad consiste en que el comportamiento del acusado se encuentra adecuado al tipo que describe la ley penal.” (Amparo directo 751/60. Simón Santillán Salazar. 29 de marzo de 1960. Unanimidad de 4 votos. Ponente: Juan José González Bustamante.

<sup>79</sup> Daza Gómez, Carlos, *Teoría General Del Delito Sistema Finalista Y Funcionalista*, 5ª. ed., México, Flores Editor y Distribuidor S.A de C.V, 2006, p. 73.

<sup>80</sup> Constitución Política de los Estados Unidos Mexicanos, nota 24.

establecer si determinado hecho encaja con el tipo legal descriptivo, y al cual se le conoce como **Juicio de tipicidad**.

De conformidad con Fernando Castellanos Tena el tipo se clasifica:

- a) Normales: Hacen una descripción objetiva.
- b) Anormales: Cuando contienen elementos objetivos y normativos, en estos últimos se hace una valoración jurídica.
- c) Fundamentales y Básicos: Sirven de esencia a otros tipos.
- d) Especiales: Agregan un requisito al tipo fundamental.
- e) Complementados: Se constituyen por un tipo básico y se agregan otro requisito.
- f) Autónomos e independientes: No dependen de otros para su existencia
- g) Subordinados: Complementan a otro tipo.
- h) De Formulación Casuística: El legislador especifica varias formas son alternativos, cuando se proveen varias hipótesis en las cuales recae el tipo y son acumulativos, porque hay concurso de hipótesis.
- i) De Formulación Amplia: Sólo establece una hipótesis y se puede llevar a cabo por cualquier medio comisivo.
- j) De daño: Los tipos tutelan a los bienes frente a una destrucción o disminución.
- k) De peligro: Se tutela el bien ante un posible daño.

Con la anterior explicación se llega a la siguiente conclusión, aunque en la Ley Penal no se prevé el Correo Electrónico Comercial no Solicitado, se hace alusión a este en la ley Federal de Protección al Consumidor. Tratare de encuadrar el siguiente ilícito en la clasificación del tipo: se habla que el Correo electrónico no Solicitado es normal, porque se está hablando de un envió no solicitado; es fundamental; es autónomo; son amplios, ya que se prevé una sola hipótesis y son de Daño, ante la posibilidad de inducir al error o confusión por engañosas o abusivas los textos, diálogos, sonidos, imágenes, entre otras denominaciones.

#### 4.2.1 Elementos objetivos del tipo penal.

Son aquellos aspectos que pueden ser perceptibles para el hombre, mismas que podemos encontrarlas en la norma jurídica. Menciona Gerardo Armando Urosa Ramírez, en su obra Teoría de la Ley Penal y del Delito, explica que “los elementos objetivos se identifican con la manifestación y proyección de la conducta descrita por el tipo penal, sea a través de una acción o una omisión, susceptible de ser valorada por el simple conocimiento, pues consiste en aquella parte de la descripción legal, apreciable a través de los sentidos –oído, gusto, olfato, la vista-, aquel fragmento de la narración legislativa que resalta “a simple vista”, y cuya concepción más elemental puede reducirse al análisis del verbo reactor que identifica la conducta típica; “sin embargo, los elementos objetivos del delito no designan sólo objetos del mundo exterior. En ellos se concluye, más bien, todo lo situado fuera de la esfera anímica del autor.”

En este sentido, se recogen como elementos objetivos la referencias, modalidades, circunstancias que forman parte de la descripción legal, siempre y cuando se refieran actos perceptibles sensorialmente por el intérprete...a la descripción gramatical objetiva depositada en el tipo está compuesta por todo aquello que se encuentra fuera de la esfera intelectual del sujeto activo y suelen ser clasificados por la doctrina en permanentes y ocasionales. A los primeros pertenece, junto con la acción: a) las calidades del sujeto activo y pasivo; a los segundos; b) el objeto jurídico y material, c) los medios utilizados, d) las referencias de lugar, tiempo, modo y ocasión, e) nexos causal y el resultado.”<sup>81</sup>

- 1) **Sujeto Activo:** es la persona física que actúa por si o en representación de una persona moral, que al manifestar su voluntad infringe un tipo penal. En este contexto se debe de analizar todo lo referente al sujeto pasivo, si la norma requiere de ciertas características que reúna el sujeto activo, el más claro ejemplo lo encontramos cuando se exige que sea un servidor o

---

<sup>81</sup> Ibídem, p.p. 111-112.

funcionario público, o bien se haga referencia en el ilícito al número de sujetos activos que intervengan en la consumación del mismo. (como se puede ver en el Código Penal Federal en su artículo 13, que habla de autoría y participación y el cual se analizará más adelante en el concurso de personas).

La Ley Federal de Protección al Consumidor, establece como sujeto activo a los proveedores de las empresas, y a los clientes de la misma sociedad, que utilicen información con fines mercadotécnicos o publicitarios.

**2) Sujeto pasivo:** Es la persona física o moral, que sufre una afectación en el bien jurídico tutelado. En algunos tipos penales también se aduce tanto a la cantidad de sujetos pasivos y a ciertas características que se exigen en la ley para que el actuar ilícito sea agotado. La Ley Federal de Protección al Consumidor se refiere al sujeto pasivo como consumidores y es claro al respecto “no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio para ofrecer bienes, productos o servicios, y que no le envíen publicidad.

**3) Medios utilizados:** Mejor conocidos como medios comisivos, son formas que exige la ley en ciertos casos para la realización del delito. En la Ley Federal de Protección al Consumidor se hace referencia en su artículo 32, a los siguientes medios:

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

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

La información o publicidad que compare productos o servicios, sean de una misma marca o de distinta, no podrá ser **engañosa o abusiva** en términos de lo dispuesto en el párrafo anterior.

La procuraduría podrá emitir lineamientos para el análisis y verificación de dicha información o publicidad a fin de evitar que se **induzca a error o confusión** al consumidor, considerando el contexto temporal en que se difunde, el momento en que se transmite respecto de otros contenidos difundidos en el mismo medio y las circunstancias económicas o especiales del mercado.<sup>82</sup>

- 4) **Referencias de tiempo, modo u ocasión:** son aquellas referencias que pueden hacer relevante el tipo penal o lo agrava.

Como lo establece el artículo 128 Bis de la Ley Federal de Protección al Consumidor haciendo referencia al artículo 32 las penas se agravaran por reincidencia, en los casos del artículo 128 Ter.

**“Artículo 128 bis.** En casos particularmente graves, la procuraduría podrá sancionar con clausura total o parcial, la cual podrá ser hasta de noventa días y con multa de \$128,643.37 a \$3,602,014.24.

---

<sup>82</sup> Ley Federal de Protección al Consumidor, nota 27.

*Las violaciones a lo establecido en el artículo 32 que se consideren particularmente graves conforme a lo establecido en el artículo 128 ter de esta ley, serán sancionadas con la multa establecida en el párrafo anterior o bien con multa de hasta un 10% de los ingresos brutos anuales del infractor obtenidos por la comercialización del bien o los bienes, productos o servicios contenidos en la publicidad respectiva, correspondiente al último ejercicio fiscal en que se haya cometido la infracción, en caso de reincidencia.”*

**“Artículo 128 ter.-** *se considerarán casos particularmente graves:*

*I. Aquellos en que de seguir operando el proveedor, se pudieran afectar los derechos e intereses de un grupo de consumidores;*

*II. Cuando la infracción de que se trate pudiera poner en peligro la vida, la salud o la seguridad de un grupo de consumidores;*

*III. Aquellas infracciones que se cometan en relación con bienes, productos o servicios que por la temporada o las circunstancias especiales del mercado afecten los derechos de un grupo de consumidores;*

*IV. Aquellas conductas que se cometan aprovechando la escasez, lejanía o dificultad en el abastecimiento de un bien o en la prestación de un servicio;*

*V. Cuando se trate de productos básicos de consumo generalizado, como alimentos, gas natural o licuado de petróleo, gasolina o productos sujetos a precio máximo o a precios o tarifas establecidos o registrados por la secretaría o por cualquiera otra autoridad competente;*

*VI. Cuando la información o publicidad relacionada con algún bien, producto o servicio que pudiendo o no ser verdadera, induzcan a error o confusión al consumidor por la forma falsa, exagerada, parcial, artificiosa o tendenciosa en que se presente;*

*VII. La reincidencia en la comisión de infracciones a los artículos señalados en el artículo 128 de esta ley, y*

*VIII. Aquellas que vulneren los derechos contemplados en el título segundo de la ley para la protección de los derechos de niñas, niños y adolescentes.*<sup>83</sup>

**5) El Nexa Causal y el Resultado:** Se habla de nexa causal ante la existencia de un enlace o vínculo, entre el actuar del agente y el resultado; este nexa causal se da únicamente en los delitos de acción y omisión simple. El resultado “consiste en el cambio en el mundo externo, físico, provocado por la manifestación de voluntad. Es la culminación de una conducta delictiva que llega a consumarse, ya sea lesionando o amenazando el bien jurídico tutelado por la norma.”<sup>84</sup>

#### **4.2.2 Elementos normativos del tipo penal.**

Estos elementos no se perciben a través de los sentidos pues la descripción legal necesita de un juicio de la apreciación o evaluación por parte del juez, para darle sentido al tipo. Para Eduardo López Betancourt: “son una llamada de atención del juez, en los que se le trata de advertir que debe confirmar la antijuridicidad de la conducta, ya que con estos elementos, un hecho aparentemente lícito puede pasar a ser un hecho ilícito, así mismo puede ocurrir lo contrario, es decir, que un hecho aparentemente ilícito no lo sea.”<sup>85</sup> Se dividen en su estudio en culturales y jurídicos:

En la Ley Federal de Protección al Consumidor respecto a los elementos:

**a) Culturales.** Según el Diccionario de la Real Academia Española<sup>86</sup> define los siguientes conceptos:

---

<sup>83</sup> Ídem, nota 24.

<sup>84</sup> Urosa Ramírez, Gerardo Armando, op. cit., nota 62, p. 117.

<sup>85</sup> Ibídem, p. 121.

<sup>86</sup> Real academia española, nota 9.

- **Bienes:** Unidad de organización dedicada a actividades industriales, mercantiles o de prestación de servicios con fines lucrativos.
- **Envió:** Hacer que algo se dirija o sea llevado a alguna parte.
- **Utilización:** Aprovecharse de algo.
- **Veraces:** Que dice, usa o profesa siempre la verdad.
- **Comprobables:** Verificar, confirmar la veracidad o exactitud de algo.
- **Extensos:** Que tiene extensión.
- **Inexacta:** Que carece de exactitud.
- **Falsa:** Incierto y contrario a la verdad.
- **Exagerada:** Decir, representar o hacer algo traspasando los límites de lo verdadero, natural, ordinario, justo o conveniente.
- **Parcial:** Perteneciente o relativo a una parte del todo.
- **Artificiosa:** Hecho o elaborado con artificio, arte y habilidad.
- **Tendenciosa:** Que presenta o manifiesta algo parcialmente, obedeciendo a ciertas tendencias, ideas, etc.
- **Servicios.** Econ. Prestación humana que satisface alguna necesidad social y que no consiste en la producción de bienes materiales.

#### b) Jurídicos:

- **Consumidores:** (art. 2.) Consumidor: la persona física o moral que adquiere, realiza o disfruta como destinatario final bienes, productos o servicios. Se entiende también por consumidor a la persona física o moral que adquiera, almacene, utilice o consuma bienes o servicios con objeto de integrarlos en procesos de producción, transformación, comercialización o prestación de servicios a terceros, únicamente para los casos a que se refieren los artículos 99 y 117 de esta ley.<sup>87</sup>
- **Proveedores.** (art. 2.) Proveedor: la persona física o moral en términos del Código Civil Federal, que habitual o periódicamente ofrece,

---

<sup>87</sup> Ley Federal de Protección al Consumidor, nota 27.

distribuye, vende, arrienda o concede el uso o disfrute de bienes, productos y servicios.<sup>88</sup>

- **Empresa.** (art.16) empresa la unidad económica de producción o distribución de bienes o servicios y por establecimiento la unidad técnica que como sucursal, agencia u otra forma semejante, sea parte integrante y contribuya a la realización de los fines de la empresa.<sup>89</sup>
- **Productos:** (art. 19. Fracción I) Productos que deban expresar los elementos, sustancias o ingredientes de que estén elaborados o integrados así como sus propiedades, características, fecha de caducidad, contenido neto y peso o masa drenados, y demás datos relevantes en los envases, empaques, envolturas, etiquetas o publicidad, que incluyan los términos y condiciones de los instructivos y advertencias para su uso ordinario y conservación.<sup>90</sup>
- **Marcas. (art. 68)** Se entiende por marca a todo signo visible que distinga productos o servicio de otros de su misma especie o clase en el mercado<sup>91</sup>
- **Denominaciones de origen. (Art. 156)** Se entiende por denominación de origen, el nombre de una región geográfica del país que sirva para designar un producto originario de la misma, y cuya calidad o característica se deban exclusivamente al medio geográfico, comprendido en este los factores naturales y los humanos.<sup>92</sup>

---

<sup>88</sup> Ídem.

<sup>89</sup> Ley Federal del Trabajo, disponible en: [http://www.stps.gob.mx/bp/micrositios/reforma\\_laboral/archivos/Noviembre.%20Ley%20Federal%20del%20Trabajo%20](http://www.stps.gob.mx/bp/micrositios/reforma_laboral/archivos/Noviembre.%20Ley%20Federal%20del%20Trabajo%20), Consultada el 19 de julio de 2012 a las 17:00 horas.

<sup>90</sup> Ley Federal de Protección al Consumidor, nota 27.

<sup>91</sup> Ley de Propiedad Industrial, disponible en: <http://info4.juridicas.unam.mx/ijure/fed/60/>, consultada el 23 de agosto de 2012 a las 14:30 horas.

<sup>92</sup> Ídem.

### 4.2.3 Elementos subjetivos del tipo penal.

Son aquellas características que cubre el sujeto activo, los cuales infringen la ley en su actuar. Para Gerardo Armando Urosa Ramírez, explica que se habla de los elementos normativos “Cuando el contenido interno de la voluntad está contemplado de manera literal en la descripción legal, ya sea evocando un especial conocimiento del sujeto activo, un específico ánimo o concreta dirección de la finalidad o su conducta, suelen denominárseles elementos subjetivos del tipo o injusto.”<sup>93</sup> En este tipo de elementos se estudia al dolo y la culpa, se encuentran consignados en el Código Penal Federal artículo 9º.

*“Obra dolosamente el que, conociendo los elementos del tipo penal, o previniendo como posible el resultado típico, quiere o acepta la realización del hecho descrito por la ley, y obra culposamente el que produce el resultado típico, que no previo siendo previsible o previo confiando en que no se produciría, en virtud de la violación a un deber de cuidado, que debía y podía observar según las circunstancias y condiciones personales.”<sup>94</sup>*

**a) Dolo:** Para Griselda Amuchategui Recona, “consiste en causar intencionalmente el resultado típico, con conocimiento y conciencia de la antijuridicidad del hecho. También se conoce como delito intencional o doloso.”<sup>95</sup> Significa querer realizar de forma consiente y voluntaria el resultado típico descrito penalmente por la ley. Aunque doctrinalmente se habla de un dolo directo, indirecto, eventual, determinado e indeterminado, en la legislación penal sólo se habla del dolo directo y eventual.

---

<sup>93</sup> Urosa Ramírez, Gerardo Amando, op. cit., nota 62, p. 129.

<sup>94</sup> Código Penal Federal, op. cit., nota 25.

<sup>95</sup> Amuchategui Requena, Griselda, op. cit., nota 73, p. 92.

- **Directo:** el actuar del sujeto activo va dirigido al resultado típico que ejecuta satisfactoriamente; se habla de una perfecta armonía entre el actuar del agente y su resultado.
- **Eventual:** en este dolo existe una probabilidad de que el resultado se logre y aunque el sujeto activo ante la representación del resultado no lo quiere, toma una postura de indiferencia y admite su producción.

En lo que respecta al correo electrónico no solicitado se habla de un dolo directo, pues de la interpretación en contrario sensu del artículo 17, 2º párrafo y 32 de La Ley Federal de Protección al Consumidor. El dolo se configura en el instante exacto, en que se envié la información con otro fin distinto al de mercadotecnia y publicidad. Cuando se le moleste en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio para ofrecerle bienes productos o servicios o bien que su información sea cedida o transmitida a terceros; por último también se da el dolo directo cuando la información relativa a bienes, productos y servicios difundida por cualquier medio no sea veras, comprobable y contenga textos, diálogos, sonidos, imágenes, marcas, denominaciones de origen y otras descripciones que induzcan a error o confusión engañosa o abusiva. Es por ello que se excluye a la culpa en este tipo de ilícitos.

**b) Culpa:** Un sujeto obra culposamente “si se estima que el resultado típico realizado fue producto de una actuación predecible por una persona común acorde a sus circunstancias.”<sup>96</sup> Para Raúl Carranca y Trujillo, “es la no previsión de lo previsible y evitable, que causa un daño antijurídico y penalmente tipificado.”<sup>97</sup> De conformidad con el artículo 9 del Código Penal Federal se habla de dos tipos de culpa: tal como lo menciona Fernando Castellano Tena.<sup>98</sup>

---

<sup>96</sup> Urosa Ramírez, Gerardo Armando, op. cit., nota 62, p. 149.

<sup>97</sup> Carranca y Trujillo, Raúl y Carranca y Rivas, Raúl, *Derecho penal mexicano*, 22ª. ed., México, Porrúa, 2004, p. 517.

<sup>98</sup> Castellanos Tena, Fernando, op. cit., nota 66, p. 251.

- **Consiente sin previsión y sin representación:** el agente prevé el posible resultado penalmente tipificado; abriga la esperanza de que éste no se producirá. Como en el dolo eventual hay voluntad de efectuar la conducta y existe representación del resultado típico, pero mientras que en el dolo eventual se asume indiferencia ante ese probable resultado, la culpa consiente se espera que no se producirá.
- **Inconsciente, sin previsión o sin representación:** el agente no prevé la posibilidad de que emerja el resultado típico, a pesar de ser previsible. No prevé lo que debió haber previsto.

Hay que destacar que en la culpa no existe la figura de tentativa como consumación del delito.

Con ello reafirmo que en el correo electrónico no solicitado, no surge la culpa con representación y culpa sin representación, no se puede hablar de un actuar negligente. Es necesario que el acto consista en el envío y utilización, es decir, un dolo directo.

- **ATIPICIDAD.**

Se habla de atipicidad cuando no exista una ley que se pueda aplicar al caso concreto o bien cuando no se presenten alguno de los elementos que integra el tipo penal, esta última hipótesis se constata en el art. 15 fracción II del Código Penal Federal.

***“Artículo 15. El delito se excluye cuando:***

***II. Se demuestre la inexistencia de alguno de los elementos que integran la descripción típica del delito de que se trate.”***

No se presenta la ausencia de tipicidad en lo que respecta al correo electrónico no solicitado, pero por encontrarse en una ley donde no se contemplan todos los medios comisivos y no se haga referencia a alguna medida relativa al Código Penal Federal, se quedara en la mayoría de los casos impune el actuar del sujeto activo.

### **4.3 Antijuridicidad.**

Existe antijuridicidad, en el momento que no está permitida por ninguna norma jurídica, pues una sola disposición que autorice la conducta típica es suficiente para poder afirmar que no existe contrariedad en el orden jurídico.

“La acción es antijurídica, cuando es contraria a Derecho y produce un resultado material o formal.”<sup>99</sup> Miguel Ángel Aguilar López se expresa en la misma idea cuando se interpreta el artículo 15 fracciones III a la VI del Código Penal Federal. Otros juristas contemplan a la antijuridicidad como “... el análisis de la antijuridicidad tiene por finalidad establecer las condiciones en las que la realización típica de un evento, pueda resultar antijurídica por no estar amparada por justificante alguna, dando lugar al estudio de otro elemento conceptual del delito o antijuridicidad.” O “lo contrario a derecho” y consiste en la reprobación jurídica que recae sobre la conducta, al cotejarla con las normas penales que integran el orden jurídico.<sup>100</sup> Para Villalobos “la infracción de las leyes significa antijuridicidad formal y el quebrantamiento de las normas que las leyes interpretan constituye la antijuridicidad material.”<sup>101</sup>

De acuerdo a la definición del autor anterior se hablan de dos tipos de antijuridicidad, formal y material:

---

<sup>99</sup> Aguilar López, Miguel Ángel, op. cit., nota 65, p. 7.

<sup>100</sup> Urosa Ramírez, Gerardo Armando, op. cit., nota 62, p.p. 180 y 194.

<sup>101</sup> Castellanos Tena, Fernando, op. cit., nota 66, p. 181.

- a) **Formal:** con el actuar del sujeto activo se violenta la norma establecida por el estado.
- b) **Material:** se da cuando se causa un daño al bien jurídico tutelado, se habla de un menoscabo a los intereses de la sociedad.

- **CAUSAS DE JUSTIFICACIÓN**

Para Luis Jiménez de Asúa, “son las razones o circunstancias que el legislador reconsidero para anular la antijuridicidad de la conducta y típica realizada, al estimarla licita, jurídica o justificativa.”<sup>102</sup>

Establecida en el artículo 15 del Código Penal Federal, son el aspecto negativo de la antijuridicidad y se presentan en los siguientes supuestos:

**“Artículo 15. El delito se excluye cuando:**

*III. Se actué con el consentimiento del titular del bien jurídico afectado, siempre que se llenen los siguientes requisitos:*

*A) que el bien jurídico sea disponible;*

*B) que el titular del bien tenga la capacidad jurídica para disponer libremente del mismo; y*

*C) que el consentimiento sea expreso o tácito y sin que medie algún vicio; o bien, que el hecho se realice en circunstancias tales que permitan fundadamente presumir que, de haberse consultado al titular, este hubiese otorgado el mismo;*

*IV. Se repela una agresión real, actual o inminente, y sin derecho, en protección de bienes jurídicos propios o ajenos, siempre que exista necesidad de la defensa y racionalidad de los medios empleados y no*

---

<sup>102</sup> Jiménez de Asúa, Luis en Amuchategui Requena, Griselda, op. cit., nota 73, p. 74.

*medie provocación dolosa suficiente e inmediata por parte del agredido o de la persona a quien se defiende.*

*Se presumirá como defensa legítima, salvo prueba en contrario, el hecho de causar daño a quien por cualquier medio trate de penetrar, sin derecho, al hogar del agente, al de su familia, a sus dependencias, o a los de cualquier persona que tenga la obligación de defender, al sitio donde se encuentren bienes propios o ajenos respecto de los que exista la misma obligación; o bien, lo encuentre en alguno de aquellos lugares en circunstancias tales que revelen la probabilidad de una agresión;*

*V. Se obre por la necesidad de salvaguardar un bien jurídico propio o ajeno, de un peligro real, actual o inminente, no ocasionado dolosamente por el agente, lesionando otro bien de menor o igual valor que el salvaguardado, siempre que el peligro no sea evitable por otros medios y el agente no tuviere el deber jurídico de afrontarlo;*

*VI. La acción o la omisión se realicen en cumplimiento de un deber jurídico o en ejercicio de un derecho, siempre que exista necesidad racional del medio empleado para cumplir el deber o ejercer el derecho, y que este último no se realice con el solo propósito de perjudicar a otro.”<sup>103</sup>*

**1) Consentimiento del titular.** (Artículo 15 fracción III del Código Penal Federal). Es una causa de justificación que elimina la integración de la antijuridicidad, porque se habla de una renuncia al interés protegido. Para que el consentimiento tenga eficacia, es necesario que tenga disponibilidad sobre el bien jurídicamente protegido. Que se tenga capacidad para poder disponer del bien, que sea tácito o expreso el consentimiento o que se actué con la presunción, que de haberse consultado al titular éste hubiera otorgado el consentimiento y último que no exista vicio alguno.

---

<sup>103</sup> Código Penal Federal, nota 25.

**2) Legítima defensa.** (Art. 15 fracción IV Código Penal Federal). Se habla de una repulsa necesaria ante una amenaza o agresión real, actual e inminente y sin derecho. Cabe destacar que debe de existir la necesidad de defensa. Para Miguel Ángel Aguilar López, es “Quien actué en defensa legítima, lleva a que su conducta sea lícita, es decir, jurídica, por la exclusión de la antijuridicidad. Pero en la medida en que la defensa sea expuesta proporcionada a una agresión injusta, no cabe duda de que, cualquiera que sea la actitud anímica del que se defiende, existe autentica causa de licitud que legitima el acto realizado.”<sup>104</sup> Edmund Mezger, menciona que “no actúa antijurídicamente el que obra en situación de legítima defensa.”<sup>105</sup> Para Franz Von Liszt, estima que “se legitima la defensa necesaria para repeler una agresión actual y contraria al derecho mediante una agresión contra el atacante.”<sup>106</sup>

Para Ignacio Villalobos, “Como elementos de la defensa legítima se señalan los siguientes:

- a) Una agresión injusta y actual.
- b) Un peligro inminente de daño, derivado de la agresión, sobre bienes jurídicamente tutelados, y
- c) Repulsa de dicha agresión.”<sup>107</sup>

**3) Estado de necesidad.** (artículo 15 fracción V del Código Penal Federal). Nos encontramos en aquellas circunstancias que realmente representan un peligro para los bienes jurídicamente tutelados de menor o igual valor, ante la necesidad de defenderlos. Eugenio Cuello Calón, lo considera como “el peligro actual o inmediato para bienes jurídicamente protegidos, que sólo puede evitarse mediante la lesión de bienes también jurídicamente tutelados, pertenecientes a otra

---

<sup>104</sup> Aguilar López, Miguel Ángel, op. cit., nota 65, p.p. 311-312.

<sup>105</sup> Mezger, Edmund, *Derecho Penal*, 2ª. ed., México, Cárdenas Editor y Distribuidor, 1990, p. 148.

<sup>106</sup> Castellanos Tena, Fernando, op. cit., nota 66, p. 191.

<sup>107</sup> Ídem.

persona.”<sup>108</sup> Gerardo Armando Urosa Ramírez, especifica que el estado de necesidad “acontece cuando ante la disyuntiva para salvaguardar un bien de mayor o igual jerarquía jurídicamente tutelado se lesiona otro bien, igualmente protegido por la ley.”<sup>109</sup>

“Estado de Necesidad, Excluyente de.” 1°Sala de la SCJN, 7°Epoca, 1969, pág. 21 del Semanario Judicial de la Federación.

ESTADO DE NECESIDAD, EXCLUYENTE DE. El estado de necesidad es una situación de peligro real e inminente, para un bien jurídicamente protegido (o pluralidad de bienes), que se salvaguardan mediante la destrucción o menoscabo de otros, siendo este, el único recurso practicable como menos perjudicial.<sup>110</sup>

De lo anterior se puede sustraer los elementos del Estado de Necesidad:

- a) Exista una situación de peligro,
- b) Que el peligro sea real e inminente,
- c) Bien este jurídicamente protegido,
- d) Y se salvaguarde un bien de igual o menor valor.

**4) Cumplimiento de un deber o ejercicio de un derecho.** (art. 15 fracción VI del Código Penal Federal). Se permite que el individuo realice determinada conducta atendiendo al cumplimiento de la norma, se establecen actos permisivos, como consecuencia del cumplimiento de un trabajo u oficio, siempre y cuando no cause un perjuicio en la esfera jurídica de otros.

---

<sup>108</sup> Ibídem p. 203.

<sup>109</sup> Urosa Ramírez, Gerardo Armando, op. cit., nota 62, p. 212.

<sup>110</sup> Ibídem, p. 213.

Al respecto Gerardo Amando Urosa Ramírez, explica que el cumplimiento de un deber se entiende cuando, “este fundamenta su licitud en la obligación de actuar exigida por el derecho, a pesar que, prima facie, pudiera aparentar que se tratase de una conducta antijurídica” y muestra la diferencia que existe entre cumplimiento de un deber y ejercicio de un derecho citando el siguiente amparo:

“Cumplimiento de un Deber o Ejercicio de un Derecho.” 1° Sala de la SCJN, 7° Época, 1973, Pág. 29 Semanario Judicial de la Federación.

**CUMPLIMIENTO DE UN DEBER O EJERCICIO DE UN DERECHO. DISTINCIÓN.** Se incide en un error técnico al equiparar el cumplimiento de un deber con el ejercicio de un derecho, pues aun cuando ambas excluyentes son justificantes, en el caso del ejercicio de un derecho se trata de una situación potestativa, en tanto que en el cumplimiento de un deber la acción es compulsoria; en el ejercicio de un derecho el sujeto puede o no ejecutar la acción y si la ejecuta queda exento de pena a virtud de que su conducta es jurídica, en tanto que el cumplimiento de un deber el gobernado está obligado a actuar.<sup>111</sup>

Con el anterior análisis de las causas de exclusión de la antijuridicidad, nos podemos percatar que él envió de mensajes electrónicos comerciales no solicitados, no se encuadra en ninguna causa de exclusión correspondiente, pues es bien sabido que se necesita necesariamente que el sujeto activo realice el envío de los respectivos mensajes, se efectúa el actuar de forma física y voluntaria, la computadora se utiliza como medio, ya que el sujeto pasivo no se encuentra presente físicamente en el momento en que se realiza la acción. Con esto se concluye el análisis de la antijuridicidad, y se da pauta al siguiente elemento positivo del delito.

---

<sup>111</sup> *Ibidem*, p. 217.

#### 4.4 Imputabilidad.

Celestino Porte Petit explica: “Para ser culpable un sujeto precisa que antes sea imputable; si en la culpabilidad..., intervienen el conocimiento y la voluntad, se requiere la posibilidad de ejercer esas facultades. Para que el individuo conozca la ilicitud de su acto y quiera realizarlo, debe tener capacidad de entender y de querer, de determinarse en función de aquello que conoce; luego actitud (intelectual y volitiva) constituye el presupuesto necesario de la culpabilidad. Por eso a la imputabilidad (calidad del sujeto, capacidad ante el derecho penal) se le debe considerar como el soporte o cimiento de la culpabilidad y no como un elemento del delito, según pretenden algunos especialistas.”<sup>112</sup> “La capacidad psíquica necesaria para comprender lo debido e indebido de un acto u omisión y poder decidirse de acuerdo a esa comprensión.”<sup>113</sup>

De la interpretación contrario sensu del art. 15, fracción VII, Código Penal Federal, se desprenden que el sujeto activo cuenta con:

- capacidad para comprender el hecho (no exista alguna enfermedad mental).
- la capacidad de conducirse conforme a dicho ordenamiento.

Al respecto Miguel Ángel Aguilar López pronuncia que: “Solo quien ha llegado a una determinada edad y no padece grandes perturbaciones psíquicas posee aquel mínimo de capacidad de autodeterminación que el ordenamiento jurídico-penal exige. A falta de la capacidad de culpabilidad, el autor puede ciertamente, actuar pero no llegar a ser culpable, ya que el hecho no responde a una actitud jurídica merecedora de desaprobación. Al conjunto de estas facultades mínimas requeridas para considerar a un sujeto culpable por haber hecho algo típico y antijurídico, se le llama imputabilidad o, más modernamente capacidad de culpabilidad.”<sup>114</sup>

---

<sup>112</sup> Castellanos Tena, Fernando, op. cit., nota 66, p. 217.

<sup>113</sup> Vergara Tejada, José Moisés, *Manual de Derecho Penal. Parte General*, México, Ángel Editor, 2002, p. 280.

<sup>114</sup> Aguilar López, Miguel Ángel, op. cit., nota 65, p. 364.

En este contexto, la persona física que envía el correo electrónico comercial no solicitado, cuenta tanto la capacidad de querer, y comprender el hecho, además de contar con la mayoría de edad requerida por la Constitución Política de los Estados Unidos Mexicanos es de 18 años; así mismo el individuo posee una habilidad en el manejo de equipos computacionales mayor al intelecto de un incapaz.

- **INIMPUTABILIDAD.**

La inimputabilidad constituye el aspecto negativo de la imputabilidad y se encuentra prevista, en el artículo 15 fracción VII del Código Penal Federal, que a la letra establece:

***“Artículo 15. El delito se excluye cuando:***

*VII. Al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquel o de conducirse de acuerdo con esa comprensión, en virtud de padecer trastorno mental o desarrollo intelectual retardado, a no ser que el agente hubiere provocado su trastorno mental dolosa o culposamente, en cuyo caso responderá por el resultado típico siempre y cuando lo haya previsto o le fuere previsible.*

*Cuando la capacidad a que se refiere el párrafo anterior solo se encuentre considerablemente disminuida, se estará a lo dispuesto en el artículo 69 bis de este código.”<sup>115</sup>*

Según Javier Jiménez Martínez, las causas generales de inimputabilidad son:

---

<sup>115</sup> Código Penal Federal, nota 25.

**a) Minoría de edad:** se requiere que el autor alcance un grado de desarrollo intelectual, madurez moral y fuerza de voluntad, de lo contrario aunque tenga voluntad para hacer y querer el hecho, no cuenta con la edad mínima requerida para ser sujeto a un proceso penal, estaríamos en presencia de menores infractores, que se someten a procedimientos especiales ante la autoridad respectiva.

**b) Estados mentales anormales:** Existen diferentes clasificaciones de estados mentales anormales además de las ya especificadas en el art. 15 fracción VII del Código Penal Federal, existe la clasificación doctrinal, y una segunda proporcionada por el Poder Judicial.

- Clasificación doctrinal:
  - ✓ Trastornos mentales orgánicos.
  - ✓ Trastornos mentales orgánicos e inorgánicos.
  - ✓ Epilepsia sistemática.
  - ✓ Trastornos de personalidad.
  - ✓ Esquizofrenia paranoide.
  - ✓ Trastornos sexuales.
  - ✓ Trastornos funcionales.
  
- Clasificación del Poder Judicial
  - ✓ Trastorno mental o desarrollo intelectual retardado.
  - ✓ Epilepsia.
  - ✓ Toxicomanía.
  - ✓ Intoxicación alcohólica o involuntaria.

Dentro de este estudio se encuentran a las *Actione Liberae In Causa* las cuales deben existir en el momento de la ejecución del hecho, sin embargo, el sujeto en ocasiones, antes de actuar de forma voluntaria o culposamente, se coloca en situación inimputable y en esas condiciones produce el delito.

En la Ley Federal de Protección al Consumidor, en su artículo 2° exige ciertas conductas con las que debe conducirse tanto el consumidor como el proveedor de bienes, productos y servicios, por consiguientes no se hace referencia a ningún incapaz o menor de edad.

#### **4.5 Culpabilidad.**

La culpabilidad se configura cuando el sujeto activo cuenta con ciertas calidades físicas y mentales mínimas requeridas en la ley, cumpliendo estas calidades y al que se le puede exigir un actuar diferente al que realizó ilícitamente. Miguel Ángel Aguilar López considera como, “el conjunto de condiciones que determinan que el autor de una acción típica, antijurídica y culpable sea penalmente responsable de la misma. Bajo estas premisas se comprende el rápido éxito, no sólo teórico, sino práctico, legislativo y jurisprudencial, que ha tenido la teoría de la culpabilidad.”<sup>116</sup> Jiménez de Asúa, “en el más amplio sentido puede definirse la culpabilidad como el conjunto de presupuestos que fundamentan la reprochabilidad personal de la conducta antijurídica.”<sup>117</sup> Fernando Castellanos Tena, “...consideramos a la culpabilidad como el nexo intelectual y emocional que liga al sujeto con su acto.”<sup>118</sup>

- **INCULPABILIDAD.**

Es considerada la excluyente de culpabilidad, porque la conducta está viciada de un error y su actuar es ilícito. “las causas de inculpabilidad eliminan alguno de los dos elementos esenciales de la culpabilidad: el intelectual y el volitivo.”<sup>119</sup> Se deriva del artículo 15 fracciones VII, VIII, IX, del Código Penal Federal.

---

<sup>116</sup> Aguilar López, Miguel Ángel, op. cit., nota 65, p. 353.

<sup>117</sup> Castellanos Tena, Fernando, op. cit., nota 66, p. 233.

<sup>118</sup> *Ibidem*, p. 234.

<sup>119</sup> Arilla Bas, Fernando, *Derecho penal. Parte general*, México, Porrúa, 2001, p. 293.

**“Artículo 15.** *El delito se excluye cuando:*

*VII. Al momento de realizar el hecho típico, el agente no tenga la capacidad de comprender el carácter ilícito de aquel o de conducirse de acuerdo con esa comprensión, en virtud de padecer trastorno mental o desarrollo intelectual retardado, a no ser que el agente hubiere provocado su trastorno mental dolosa o culposamente, en cuyo caso responderá por el resultado típico siempre y cuando lo haya previsto o le fuere previsible.*

*Cuando la capacidad a que se refiere el párrafo anterior solo se encuentre considerablemente disminuida, se estará a lo dispuesto en el artículo 69 bis de este código.*

*VIII. Se realice la acción o la omisión bajo un error invencible;*

*A) sobre alguno de los elementos esenciales que integran el tipo penal; o  
B) respecto de la ilicitud de la conducta, ya sea porque el sujeto desconozca la existencia de la ley o el alcance de la misma, o porque crea que está justificada su conducta.*

*Si los errores a que se refieren los incisos anteriores son vencibles, se estará a lo dispuesto por el artículo 66 de este código;*

*IX. Atentas las circunstancias que concurren en la realización de una conducta ilícita, no sea racionalmente exigible al agente una conducta diversa a la que realizo, en virtud de no haberse podido determinar a actuar conforme a derecho.”<sup>120</sup>*

Así encontramos los siguientes tipos de error: El delito se excluye cuando se realice la acción o la omisión bajo un error invencible:

---

<sup>120</sup> Código Penal Federal, nota 25.

- 1) **Error de tipo** (artículo 15 fracción VIII inciso A del Código Penal Federal). En ésta el sujeto activo cree que su actuar no es contrario a derecho, hay un desconocimiento de los elementos normativos del tipo, el dolo es querer por tanto aunque se quiera si se desconoce los elementos normativos del tipo, se habla de error de tipo invencible, y elimina tanto al dolo como a la culpa, en cambio el error de tipo vencible, la culpa se caracteriza por ser negligente por tanto se debía tener un deber de cuidado, así en el tipo vencible se elimina al dolo mas no a la culpa, según requiera de esta figura el tipo penal.
  
- 2) **Error de prohibición** (artículo 15 fracción VIII inciso B del Código Penal Federal). Es aquel que maneja una apreciación equivocada de la verdad por el desconocimiento de la norma jurídica, en el error de prohibición directo, se cree que existe un una causa de justificación de la norma, es decir su actuar está justificado, y en el error de prohibición indirecto, hay ignorancia sobre la existencia del tipo, o bien se realiza creyendo que el actuar no está prohibido por la ley, en este caso se puede hacer mención, que la cultura o costumbres son muy diferentes y varían sus usos y costumbres, algunas veces por ello el actuar para ellos es normal, o bien por ser pueblos aislados desconocen la ley vigente.
  
- 3) **La no exigibilidad de otra conducta.** La última excluyente de conformidad con el art. 15 fracción IX del Código Penal Federal, en ella mediante la realización de un juicio se llega a la conclusión que el sujeto activo se pudo haber dirigido su actuar de forma diferente, y con él se halla evitado el resultado ilícito de la conducta. Gerardo A. Urosa Ramírez, abunda en cuanto a este tema aclarando que “La ley no puede exigir comportamiento heroicos extremos. El juez debe utilizar la empatía como método para sopesar el grado de exigibilidad o su ausencia, atento a las circunstancias y condiciones concretas del individuo, al momento de acontecer el hecho que ocasiono su actuar en determinado sentido.

Haciendo de lado posibles circunstancias que pudieran orillar al agente a actuar, en determinada dirección una persona común y corriente, con capacidad para comprender en carácter antijurídico del hecho que realiza o conducirse conforme a ésta y con conocimiento sobre su significación antijurídica, le será racionalmente exigible un comportamiento apegado a derecho, y en su caso contrario podrá censurarse penalmente su actuar.<sup>121</sup>

Los supuestos de exigibilidad de otra conducta reconocidos doctrinalmente son:

- a) El estado de necesidad disculpante: Al igual que el estado de necesidad se habla de repeler una agresión real, actual e inminente en defensa de un bien jurídico propio o ajeno, sin embargo la diferencia se encuentra en que el bien jurídico que se lesiona o se causa daño es de igual valor, y no de menor valor como en el estado de necesidad. Por lo tanto alguno de los dos bienes se daña.
- b) El miedo grave y el temor fundado: Ambas se originan dentro del psique del humano, son estados psicológicos, pero su diferencia se hacen notar, cuando el miedo grave provoca una perturbación tan aguda que impide incluso el mismo actuar de la persona, es una exteriorización del sujeto de dentro hacia afuera; el temor fundado en cambio, se induce de afuera hacia adentro, logrando que el sujeto exteriorice su voluntad conduciendo su conducta hacia un actuar ilícito, ante la amenaza presentada.

No se presenta ninguna excluyente de culpabilidad, porque el sujeto cuenta con todas las capacidades requeridas en la ley, además, el proveedor cuando actúa por sí o a nombre de la empresa, debe tener pleno conocimiento de la conducta prohibida, que en este caso es el envío de correo comercial no

---

<sup>121</sup> Urosa Ramírez, Gerardo Armando, op. cit., nota 62. Pág. 257.

solicitado, por tanto no se da el error de tipo, ni el de prohibición, así como tampoco la exigibilidad de otra conducta.

#### **4.6 Punibilidad.**

La punibilidad es la aplicación de la sanción o de las medidas de seguridad que corresponde al caso en concreto, como consecuencia de un actuar típico, antijurídico y culpable, para muchos autores se considera una amenaza que el Estado realiza al sujeto activo con la intención que éste no actué ilícitamente, de lo contrario ante el ilícito será punible.

Hablar de punibilidad es hablar de sanción. La sanción, es la aplicación de medidas establecidas en la ley, las cuales pueden variar en grado, es decir, dependiendo del actuar del sujeto activo será su sanción, les habla de diferentes medidas, entre las que encontramos las pecuniarias, administrativas o de privación de la libertad.

En la Ley Federal de Protección al Consumidor,<sup>122</sup> en lo que respecta a los correos electrónicos comerciales no solicitados, sólo establece penas pecuniarias para los casos en que las empresas utilicen la información personal del consumidor con fines fuera de los mercadotécnicos o publicitarios; o en el caso del artículo 32, cuando los textos, diálogos, sonidos, imágenes, marcas, denominaciones de origen y otras descripciones que induzcan o puedan inducir a error o confusión por engañosas o abusivas; no se da ninguna excusa absolutoria.

***“Artículo 127. Las infracciones a lo dispuesto por los artículos 7 bis, 13, 17, 18 bis, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 45, 47, 48, 49, 50, 52, 53, 54, 55, 57, 58, 59, 60, 61, 62, 66, 67, 68, 69, 70, 72, 75, 77,***

---

<sup>122</sup> Ley Federal de Protección al Consumidor, nota 27.

78, 79, 81, 82, 85, 86 quater, 87 bis, 90, 91, 93, 95 y 113 serán sancionadas con multa de \$428.81 a \$1,372,195.89.

**Multa actualizada dof 21-12-2011, 31-12-2012 con multa de \$617.41 a \$2'414,759.14.”**

**“Artículo 128 bis.** *En casos particularmente graves, la procuraduría podrá sancionar con clausura total o parcial, la cual podrá ser hasta de noventa días y con multa de \$128,643.37 a \$3,602,014.24.*

*Las violaciones a lo establecido en el artículo 32 que se consideren particularmente graves conforme a lo establecido en el artículo 128 ter de esta ley, serán sancionadas con la multa establecida en el párrafo anterior o bien con multa de hasta un 10% de los ingresos brutos anuales del infractor obtenidos por la comercialización del bien o los bienes, productos o servicios contenidos en la publicidad respectiva, correspondiente al último ejercicio fiscal en que se haya cometido la infracción, en caso de reincidencia.”*

**“Artículo 128 ter.-** *se considerarán casos particularmente graves:*

*VI cuando la información o publicidad relacionada con algún bien, producto o servicio que pudiendo o no ser verdadera, induzcan a error o confusión al consumidor por la forma falsa, exagerada, parcial, artificiosa o tendenciosa en que se presente.”*

- **EXCUSAS ABSOLUTORIAS.**

Aunque la conducta es típica, antijurídica y culpable no es sancionable, por la existencia de excusas absolutorias, éstas son de circunstancias personales del autor, se encuentran consagradas en la ley y su efecto es eliminar las penas. Para Gerardo Armando Urosa Ramírez, “las excusas absolutorias son de índole estrictamente personal, se encuentran expresamente señaladas en el texto de la

ley e impiden la sanción del delito por razones de utilidad pública o criminales.”<sup>123</sup> José Vergara Tejada, “excluyen a la punibilidad, esto es, desaparece la amenaza de la pena, aun cuando el delito se halla cometido. En este caso, el delito existe pero no puede castigarse con una pena, a virtud de causas político- sociales.”<sup>124</sup> Ejemplo de ello, cuando se da el encubrimiento de parte de familiares del delincuente por tenerle respeto, amor etc.

#### **4.7 Fases de Ideación del delito y consumación.**

El delito se realiza en un lapso de tiempo, que va desde el momento en que es concebido como, una mera idea por parte del sujeto activo hasta su consumación esto es conocido como “el camino del delito”, por este delito pasan todos los delitos dolosos, pero no se da en la culpa, el delito culposo surge en el momento en que no se tienen precauciones de lesionar al bien jurídico, por ello en ese momento se da la ejecución misma. Existen diferentes fases del camino del delito:

- a) Fase interna: encontramos a la idea criminosa o ideación (se da en la mente humana como una idea de delinquir, en ella el agente puede aceptar o no la conducta), la deliberación (en ésta se amerita la idea criminosa contra las fuerzas morales religiosas y sociales), si persiste la idea se da paso a la resolución (después de pensar, el individuo desea llevar a la practica el delito), estas se dan sólo en el pensamiento.
- b) Fase externa: comprende la manifestación (la idea surge en el mundo exterior o como exteriorización del pensamiento), preparación (son las actividades que se pueden realizar antes de la consumación del delito, pero no ponen en peligro el bien jurídico) y la ejecución (terminación del camino del delito), ésta última se da en dos hipótesis:

---

<sup>123</sup> Urosa Ramírez, Gerardo Armando, op. cit., nota 62, p.p. 285-286.

<sup>124</sup> Vergara Tejada, José Moisés, op. cit., nota 113, p. 369.

- **Tentativa:** “entendemos, pues, por tentativa los actos ejecutivos (todos o algunos), encaminados a la realización de un delito, si este no se consuma por causas ajenas al querer del sujeto”<sup>125</sup> Existen dos tipos de tentativa:
  - ✓ Acabada: a pesar de que el agente realiza todos los medios empleados, para la realización del ilícito, este no se consume por causas ajenas a su voluntad.
  - ✓ Inacabada: el agente omite alguno de los actos tendientes a la producción del resultado, ocurriendo que no se consume el delito.
  
- **Consumación:** es la ejecución de que cumple con todos los elementos del tipo penal.

#### 4.8 Concurso de personas y de delitos.

En lo que respecta al concurso de personas este surge cuando en un ilícito sin que en el tipo penal se requiera, puede existir la voluntaria cooperación de varios individuos. A continuación se explicarán los diferentes tipos de autor y los tipos de participación.

**“Artículo 13.** *Son autores o partícipes del delito:*

*I. Los que acuerden o preparen su realización. (Autor intelectual).*

*II. Los que los realicen por sí; (autoría directa o material).*

*III. Los que lo realicen conjuntamente;(coautoría).*

*IV. Los que lo lleven a cabo sirviéndose de otro;(autor mediato).*

*V. Los que determinen dolosamente a otro a cometerlo; (participe inductor).*

*VI. Los que dolosamente presten ayuda o auxilien a otro para su comisión;(cómplice).*

---

<sup>125</sup> Castellanos Tena, Fernando, op. cit., nota 66, p. 287.

*VII. Los que con posterioridad a su ejecución auxiliien al delincuente, en cumplimiento de una promesa anterior al delito y (complicidad Correspectiva).*

*VIII. Los que sin acuerdo previo, intervengan con otros en su comisión, cuando no se pueda precisar el resultado que cada quien produjo.*

*Los autores o partícipes a que se refiere el presente artículo responderán cada uno en la medida de su propia culpabilidad.*

*Para los sujetos a que se refieren las fracciones vi, vii y viii, se aplicara la punibilidad dispuesta por el artículo 64 bis de este código.”<sup>126</sup>*

El correo electrónico comercial no solicitado puede darse en autor mediato, autor directo.

Respecto al concurso de delitos, en ocasiones el autor puede ocasionar múltiples infracciones penales, esto se le denomina concurso del delito.

Estos mismos se divide en:

- Ideal: cuando el autor con un solo actuar recae en varios ilícitos penales, ocasionando daño a varios bienes jurídicos tutelados.
- Material: existen vario bienes jurídicos tutelados dañados o lesionados, porque el sujeto activo realiza varias conductas de acción u omisión.

---

<sup>126</sup> Código Penal Federal, nota 25.

## CAPÍTULO V

### EL PROBLEMA DE LA AUSENCIA DE UN TIPO PENAL, EN EL CÓDIGO PENAL FEDERAL QUE SANCIONE EL CORREO SPAM.

Como puede observarse el Estado ha realizado intentos legislativos para regular las conductas, como resultado del correo electrónico comercial no solicitado, claramente al analizarlas nos enfrentamos con muchas dudas sin respuestas.

El Código Penal Federal <sup>127</sup> hace mención en cuanto a medios electrónicos en su apartado denominado: Acceso ilícito a sistemas y equipos de informáticos. Mismos que abarcan desde el Artículo 211-bis 1 hasta el Artículo 211 bis 7, sólo mencionare algunos:

*“**Artículo 211 bis 1.** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

*Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.”*

*“**Artículo 211 bis 2.** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.*

---

<sup>127</sup> Ibidem, nota 25.

*Al que sin autorización conozca o copie información contenida en **sistemas o equipos de informática** del estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*

*A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de **almacenamiento informáticos** de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el distrito federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.”*

*“**Artículo 211 bis 3.** Al que estando autorizado para acceder a **sistemas y equipos de informática** del estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.*

*Al que estando autorizado para acceder a **sistemas y equipos de informática** del estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.*

*A quien estando autorizado para acceder a **sistemas, equipos o medios de almacenamiento informáticos** en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el*

*distrito federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.”*

*“**Artículo 211 bis 4.** Al que sin autorización modifique, destruya o provoque pérdida de información contenida en **sistemas o equipos de informática** de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.*

*Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.”*

*“**Artículo 211 bis 5.** Al que estando autorizado para acceder a **sistemas y equipos de informática** de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.*

*Al que estando autorizado para acceder a **sistemas y equipos de informática** de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.*

*Las penas previstas en este artículo se incrementarían en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero”.*

Como podemos observar dicha legislación no hace mención en ningún apartado al correo electrónico comercial no solicitado, y en dichos presupuestos legales, sólo se refiere a conceptos computacionales, a los sistemas y equipos informáticos sin brindarnos que es lo que abarca o cuál es su definición clara, para un mayor entendimiento; por tal motivo es necesario incluir una nueva ley que regule dichos envíos a través de la red, pero sobre todo se imponga una sanción equivalente al daño ocasionado. A su vez Gabriel Cámpoli, hace referencia a “la extraña exclusión que se hace de los accesos por encima de lo no autorizado al conocer o copiar, ya que se protege en este caso a las instituciones financieras y al Estado mas no a los particulares, cuando en rigor de verdad de estas conductas se producen con mayor frecuencia en equipos de empresas particulares que en las del Estado.”<sup>128</sup>

Ahora partiendo en el mismo orden de ideas observaremos la Constitución Política de los Estados Unidos Mexicanos, como la Ley Suprema en nuestra legislación vigente, en el numeral Artículo 16 señala lo siguiente:

*“**Artículo 16.** Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.*

*Toda persona tiene derecho a la **protección de sus datos personales, al acceso, rectificación y cancelación de los mismos,** así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el*

---

<sup>128</sup> Cámpoli, Gabriel Andrés, *Delitos informáticos en la legislación mexicana*, México, Instituto Nacional de Ciencias Penales, INACIPE, 2005, p. 99.

*tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.”<sup>129</sup>*

Lamentablemente dicho concepto sólo protege datos personales, pero en cuanto a lo concerniente del tema, no se regula o simplemente no se contempla al correo electrónico o dirección electrónica, es decir, difícilmente encontraremos términos, conceptos de índole informática. Aunque es importante proteger a los datos personales, al momento de utilizar y vulnerar el correo electrónico, no sólo se puede extraer los mismos, sino se puede perder información, o incluso dañar al equipo informático, por tanto considero importante que se establezcan las modalidades, en una ley especial bajo las que va operar esta protección.

## **5.1 Fortalezas y Debilidades de que la incompleta regulación en materia de Spam se encuentre en la Ley Federal de Protección al Consumidor.<sup>130</sup>**

- **La Ley Federal de Protección al Consumidor.**

*“**Artículo 17.-** en la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la **dirección electrónica** del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la procuraduría.*

*El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, **dirección electrónica** o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le **envíen publicidad**.*

---

<sup>129</sup> Constitución Política de los Estados Unidos Mexicanos, nota 24.

<sup>130</sup> Ley Federal de Protección al Consumidor, nota 27.

*Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.”*

*“**Artículo 18.-** la procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por **correo electrónico** a la procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito.”*

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

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

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

*La información o publicidad que compare productos o servicios, sean de una misma marca o de distinta, no podrá ser engañosa o abusiva en términos de lo dispuesto en el párrafo anterior.*

*La procuraduría podrá emitir lineamientos para el análisis y verificación de dicha información o publicidad a fin de evitar que se induzca a error o confusión al consumidor, considerando el contexto temporal en que se difunde, el momento en que se transmite respecto de otros contenidos difundidos en el mismo medio y las circunstancias económicas o especiales del mercado.”*

Esta legislación la hemos tomado como soporte de nuestra investigación, puesto que hace referencia al correo electrónico, mismo que lo denomina como la “dirección electrónica”; considero este aspecto como un importante elemento, puesto que éste, forma parte de la identidad de las personas, ya sean físicas y/o morales.

**a) ASPECTOS POSITIVOS.**

- Contempla al correo electrónico.
- No permite que se envíe publicidad.
- Se puede exigir, que los datos personales no sean difundidos.
- De cierta manera exige que la información se transmite sea autentica.
- No solo sanciona a personas físicas, sino también personas morales.
- Cuenta con la mayoría de los medios comisivos.

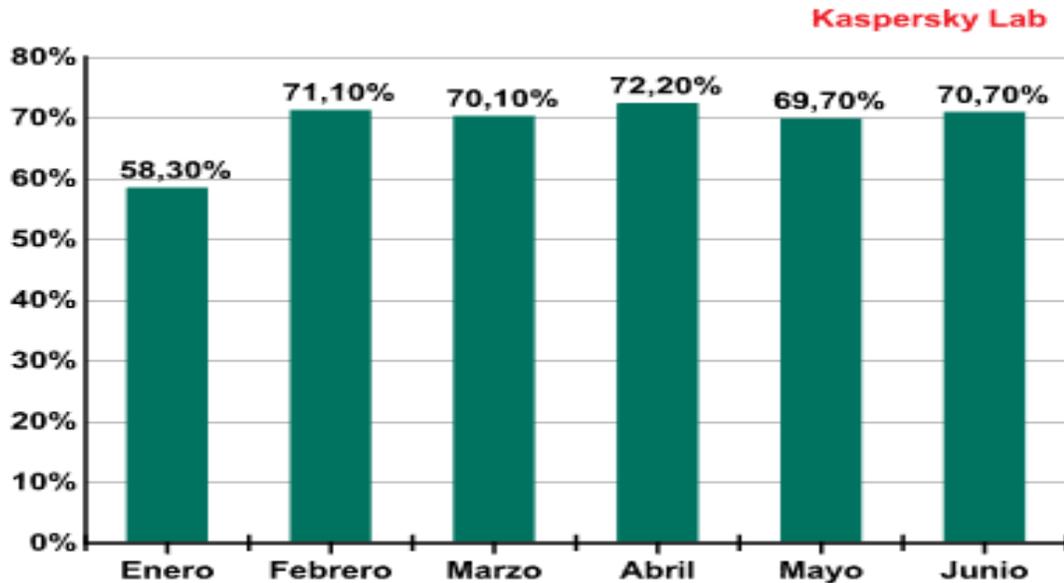
## **b) ASPECTOS NEGATIVOS.**

- El término de correo electrónico comercial no solicitado, comúnmente denominado “Spam”, no aparece en la legislación.
- Son muy pocos los artículos en donde se menciona a la dirección electrónica, por lo tanto no abarca muchos aspectos para regular y sancionar.
- No existe una verdadera seguridad para el consumidor final, porque aunque las penas pecuniarias son excesivamente altas, no hay ninguna pena de prisión.
- No existe un organismo, capaz de combatir al correo electrónico no solicitado.
- Tampoco obliga a las empresas a cumplir con lo establecido.
- No hace referencia al Código Penal Federal.

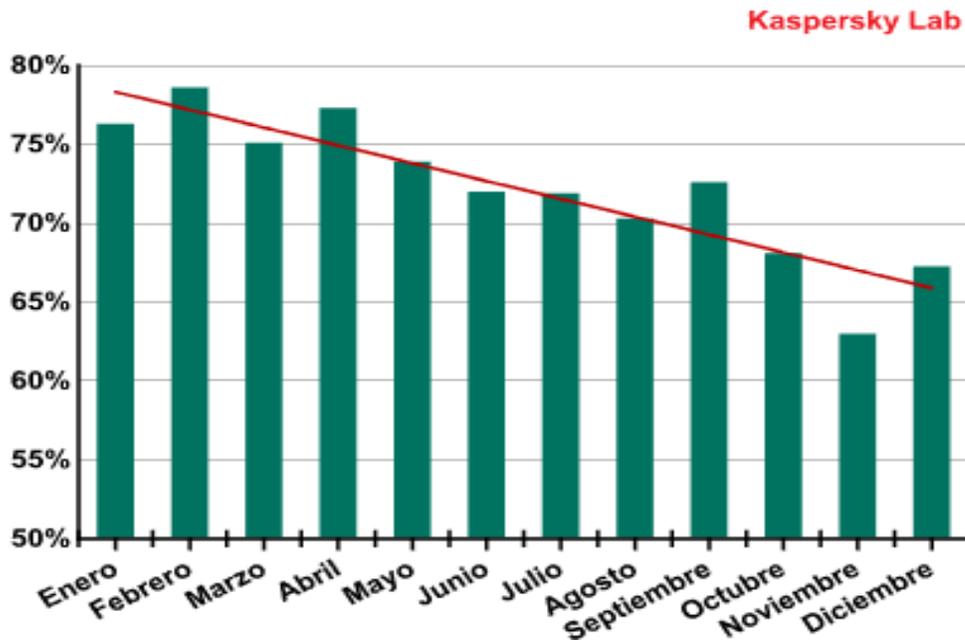
## **5.2 Importancia de realizar una Ley Anti-Spam.**

- **Incidencia del Spam:** A continuación mostrare unas gráficas con datos anuales, para observar las variaciones que se presentan en el correo electrónico comercial no solicitado y el gran impacto que representa en el tráfico de correo electrónico.

**DATOS OBTENIDOS EN EL 2013.**  
**(PORCENTAJE ES DE 73%).<sup>131</sup>**



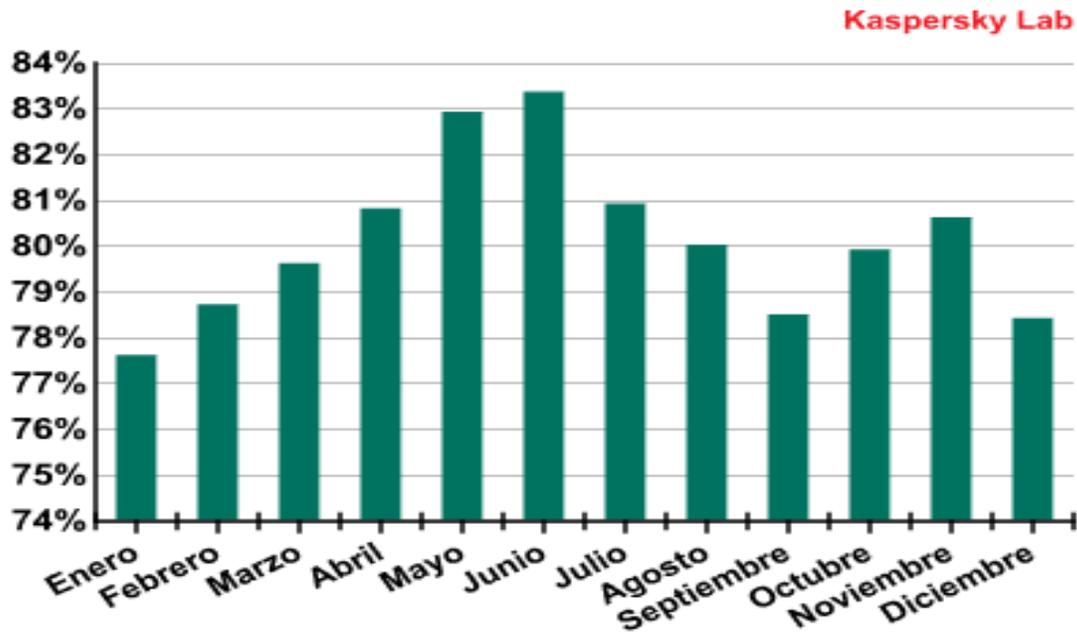
**DATOS OBTENIDOS EN EL 2012.**  
**(PORCENTAJE FUE DE 72%).<sup>132</sup>**



<sup>131</sup> Kaspersky Lab. Disponible en: <http://www.viruslist.com/sp/analysis?pubid=207271221>, consultada el 4 de julio de 2013 a las 11:00 horas.

<sup>132</sup> Kaspersky Lab. Disponible en: <http://www.viruslist.com/sp/analysis?pubid=207271199>, consultada el 12 de diciembre de 2012 a las 13:00 horas.

**DATOS OBTENIDOS EN EL 2011.  
(PORCENTAJE FUE DE 83%).<sup>133</sup>**



Como podemos observar el Spam sigue apareciendo en nuestras bandejas de entrada de correos y medio electrónicos, ya que éste no se ha podido erradicar o detener, inclusive se muestra que en años recientes, seguimos siendo víctimas tanto los usuarios como las empresas, es decir, somos muy vulnerables ante los ataques en la red.

El luchar diariamente con el Spam no es nada fácil, ya que representa para estos sectores, pérdidas no sólo de tiempo sino también de cuestiones económicas, las cuales pueden alcanzar cifras millonarias, esto se origina porque el tiempo que se ocupa en borrar cada mensaje en los correos electrónicos de aquellas grandes compañías, bien se podría ocupar para las distintas actividades de la empresa.

<sup>133</sup> Kaspersky Lab. Disponible en: <http://www.viruslist.com/sp/analysis?pubid=207271164>, consultada el 17 de octubre de 2012 a las 12:00 horas.

Así mismo, cuando estamos en presencia del correo electrónico comercial no solicitado, lamentablemente nuestros equipos de cómputo estarán en un enorme riesgo, esto debido a que en su mayoría la información contenida en estos correos, no viene sola porque en el momento de en qué accedemos a estos, nuestras computadoras serán infectadas por algún tipo de virus o datos maliciosos (*malware*).

Dichos ataques que recibimos en nuestros sistemas de cómputo, que en su mayoría se dan de manera instantánea y que estos, no son perceptibles para nosotros, cuya finalidad es convertir a nuestra computadora como una de las principales máquinas, para enviar de forma masiva al correo electrónico comercial no solicitado, es decir, nosotros estaremos realizando dicha actividad sin tener el conocimiento o la voluntad de hacerlo (computadoras zombis).

### **5.3 Tipos de Spam más recurrentes en México que deben de contemplarse en la Ley Anti-Spam.**

Algo que no debemos olvidar sobre este tipo de correos electrónicos comerciales no solicitados, es que sus métodos, temas, campos de aplicación, es muy variable y vanguardista.

Con el avance revolucionario de medios electrónicos, va de la mano con nuevas tecnologías y por lo tanto nuevas modalidades de Spam, se presentan en Celulares, Correo Electrónico y las Redes Sociales, no son la excepción, dichas figuras son las siguientes:

- **Spam Telefónico:**

Este aspecto es el más novedoso en cuanto a la investigación realizada, surge al momento en que recibimos mensajes de texto, refiriéndose a cualquier tema, en el cual nos notifican que hemos sido ganadores. Es

importante señalar que estos también son enviados masivamente y que cada vez se presenta con mucho más fuerza, ya que no hay una norma clara y contundente para frenar este delito, mismo que seguirá apareciendo en nuestros teléfonos móviles, y que estos mismos son enviados por nuestras propias compañías telefónicas o son proporcionados a las empresas de marketing que soliciten nuestros números telefónicos, que se encuentran en dicha base de datos.

- **Telemarketing:**

Su método de operar básicamente es en el área de las ventas de algún bien o servicio a través de llamadas telefónicas, algunos países lograron erradicarlo, en cuanto a México en donde sigue surgiendo es la base de datos de algunas sucursales bancarias, ya que su cartera de clientes es enorme, dándonos a conocer sus promociones financieras. En esta índole surgió una figura denominada, Registro Público de Usuarios Personas Físicas (REUS), la cual restringe a las instituciones bancarias para llamar a sus clientes por meras cuestiones publicitarias.

- **Redes Sociales:**

Actualmente con la aparición de redes sociales en Internet, (tales como *Facebook, Twitter*), han sufrido ataques en sus plataformas y las víctimas del Spam son los dueños de estas empresas mundiales y los usuarios de las mismas, ya que sus claves o contraseñas de acceso serán robadas, dando lugar al llamado Phishing (aspecto abarcado en el capítulo segundo).

- **Códigos QR:**

Esta modalidad se presenta en los comúnmente denominados “teléfonos inteligentes”, que a pesar de su avanzada tecnología también sufren ataques de Spam, en lo referente a los códigos QR, se basan en una lectura de código diseñada en un cuadrado relleno de distintos puntos, los cuales solo este tipo de teléfonos puede leer, el objetivo de anuncios que utilizan estos

código, es que al leer este código nos aparece instantáneamente el sitio de la página de Internet, que hace alusión a la publicidad que nos interesa, el Spam aquí funciona dirigiéndonos a otro sitio en Internet diferente al oficial, haciéndonos caer en el engaño, mostrándonos publicidad y posiblemente sufriremos los ataques de Spam, en ésta nueva modalidad.

Ejemplo de ello:



- **Marketing Digital:**

Una de las grandes ventajas de Internet que ha favorecido al sector empresarial es el ofrecer un bien o servicio mediante técnicas y estrategias, que versan sobre cualquier tema, servicio, producto o marca, vía correo electrónico, foros, redes sociales, etcétera. A diferencia del marketing comercial, el marketing digital da una publicidad más personalizada, con características e imágenes más específicas acerca de lo que se ofrece, para atraer la atención del usuario interesado en la adquisición del bien o servicio.

Lamentablemente nuestro país es el blanco perfecto de ataques cibernéticos de los spammer's, gracias a que la gran mayoría de la población ocupa Internet de forma muy activa en toda América Latina, cifras del 2013 señalan que México es el país número uno con más ataques en esta región y el número nueve a nivel mundial, esta información es muy preocupante pues en el 2011 ni siquiera aparecíamos en el top 20.

Con las cifras anteriores podemos constatar el inmenso incremento en la conectividad de los usuarios de nuestro país que utilizan Internet y acceden de manera constante a las diferentes redes sociales, los internautas mexicanos que utilizan Twitter, ocupan el séptimo lugar a nivel mundial y los que utilizan Facebook, ocupan el quinto lugar a nivel mundial, siendo estas plataformas las más atacadas actualmente por los bajos costos de espacios para publicidad; existen cerca de 45 millones de internautas, por lo que México es un área estratégica. Se estima que los dispositivos móviles como teléfonos inteligentes y tabletas electrónicas, son aquellas plataformas que en 2013 sufrirán más ataques de esta índole porque la gran mayoría de las personas pueden adquirirlos y tendrán acceso a servicio de Internet.

Al referirnos al Spam, estamos tratando con un tema serio, por lo cual no lo debemos tomar a la ligera, aunque se desconozcan los alcances del mismo; al observar los datos e información obtenida durante la presente investigación, los daños que ocasiona son diversos y de gran magnitud, ejemplo de ello es el tráfico en la red, es decir, alentar el sistema, perjudicar nuestros dispositivos y equipos electrónicos, incluso robar nuestra identidad y causar pérdidas monetarias de los usuarios, entre otros.

Los mensajes electrónicos no solicitados cada vez son más sofisticados, novedosos y creativos, entre ellos encontramos:

- Recibir un citatorio, para una audiencia en nuestra contra, que al acceder a dicha información se instalara un archivo en el equipo electrónico, cuyo propósito es obtener datos de nuestra cuenta bancaria.
- Un programa malicioso bloqueará nuestra computadora o dispositivo móvil, haciéndonos saber por mensajes de la policía, que nos hemos infiltrado en sitios del gobierno o realizamos descargas ilegales y cuya finalidad es presionar a la víctima, a cambio de dinero para poder restaurar su equipo electrónico y se anulara la infracción correspondiente.

- Es referente a los pagos actuales y/o pendientes, con la Comisión Federal de Electricidad (CFE)<sup>134</sup>, es muy tentador ya que la información es casi autentica y muchos aprovecharíamos grandes descuentos que nos ofrecen, lo único que se pide es, que tienen que ser pagos en línea y nos condonaran hasta la mitad de nuestra deuda.



<sup>134</sup> Disponible en: <http://www.cronicahidalgo.com/2013/05/advierte-cfe-sobre-posibles-fraudes-en-linea-para-pagos/>, consultada el 20 de mayo de 2013 a las 16:00 horas.

- Existen datos que el Sistema de Acción Tributaria (SAT)<sup>135</sup>, órgano desconcentrado de la Secretaría de Hacienda y Crédito Público (SHCP), ha detectado ataques con respecto a los contribuyentes, ya que estos reciben información falsa a nombre de esta institución, a través de llamadas telefónicas, cartas y/o correos electrónicos, los cuales hacen mención de ciertas irregularidades del contribuyente y por lo mismo es necesario regularizarse para evitar acción legal en su contra.



## COMUNICADO

Estimado(a):

La dependencia está solicitando a bancos información sobre los plásticos de sus clientes, incluso de aquellos que no tienen ningún adeudo o crédito fiscal en firme.

El artículo 32 B señala que los bancos pueden dar información de sus clientes al SAT sólo cuando éste se encuentre en proceso de comprobación para cobrar adeudos fiscales. Sin embargo, el artículo 42-A establece que la autoridad fiscal puede recabar información de terceros para iniciar una facultad de comprobación.

Por este motivo se han detectado **IRREGULARIDADES** en la consistencia de su información y SAT está alertando a los usuarios a realizar sus contribuciones adecuadamente.

Por tal motivo le pedimos llenar el formulario y evitar acciones legales para que a partir de la fecha se archive su información y UD. se comprometa a cumplir los pagos sin penalidades.



[VER FORMULARIO](#)

Av. Hidalgo 77, col. Guerrero, c.p. 06300, México, D.F. Atención telefónica 01 800 46 36 728, desde Estados Unidos y Canadá 1 877 44 88 728.

<sup>135</sup> Disponible en: [ftp://ftp2.sat.gob.mx/asistencia\\_servicio\\_ftp/publicaciones/sindicos/alertacorreosapocrifos.pdf](ftp://ftp2.sat.gob.mx/asistencia_servicio_ftp/publicaciones/sindicos/alertacorreosapocrifos.pdf), consultada el 7 de julio de 2013 a las 17:00 horas.

A continuación hago mención de un listado realizado por la dependencia, ya que ha logrado localizar ciertos correos electrónicos cuyo contenido es referente a información falsa, es decir, estamos siendo atacados por Spam:

<b>admins@telcel.com</b>	aduanademexicosat@hotmail.com
<b>aduanamexicojw@live.com.mx</b>	alertas@shcp.gob.mx
<b>alertas@shcp-gob.mx</b>	avisos@shcp-sat.mx
<b>avisos@hacienda.gob.mx</b>	avisos@sat-gob.mx
<b>avisos@sat.gob.mx</b>	avisos@sat-hacienda.gob.mx
<b>avisos@shcp.gob.mx</b>	avisos@shcp-gob.mx
<b>avisosat@shcp.gob.mx</b>	boletin@hacienda.gob.mx
<b>boletines@sat.gob.mx</b>	cobranzas@sat.gob.mx
<b>comunica@sat.com.mx</b>	comunicados_dir@sat.gob.mx
<b>contacto@sat.com.mx</b>	contacto@shcp.com
<b>contacto@shcp.gob.mx</b>	contraloria@hacienda.com.mx
<b>contraloria@hacienda.gob.mx</b>	contraloria@sat.com.mx
<b>declarasat@sat.gob.mx</b>	denuncia-sat@hotmail.com
<b>impuestos@sat.gob.mx</b>	info@taxrefund2010.com.mx
<b>informa@shcp.com.mx</b>	noreplay@shcp.com.mx
<b>notassav@shcp.gob.mx</b>	notificaciones@notificaciones.santander.com.mx
<b>notificaciones@shcp.gob.mx</b>	obligacionesfiscales@sat.gob.mx
<b>recaudaciones@sat.mx</b>	recaudadora@sat.gob.mx
<b>recursoshumanossat@hotmail.com</b>	sat.in_forma@hotmail.com
<b>sat@shcp.gob.mx</b>	sat@shcp.org.mx
<b>sat@telcel.com</b>	sat.shcp@mail.telcel.com
<b>secretariadeadministraciontributaria.cobranza@sat.com.mx</b>	shcp@mail.telcel.com
<b>shcp-sat@mail.telcel.com</b>	ventanilla@sat.gob.mx

También se han detectado mensajes de direcciones electrónicas, supuestamente, bancarias que hacen referencia a la situación del contribuyente ante el SAT, estos mensajes son apócrifos si tienen el siguiente remitente:

**newsletter@informa.santander.com.mx**

- Las instituciones bancarias no son la excepción, ya que está circulando en la red una serie de correos electrónicos a nombre de Bancomer, Banamex, Santander, etc., tarjetas de Crédito Visa y/o MasterCard; el objetivo es obtener datos personales e información confidencial. para dar paso a diversas acciones fraudulentas como lo es el phishing, dicha alerta es lanzada a los cuentahabientes por la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).<sup>136</sup>
- Sitios en internet que son falsos:



<sup>136</sup> Disponible en: <http://www.aguadigital.com/metro/leer.php?idnota=41409>, consultada el 17 de octubre de 2012 a las 12:00 horas.

- ✓ [www.banamex.com.mx/esp/contactenos.html](http://www.banamex.com.mx/esp/contactenos.html).
  - ✓ [www.banamex.com.mx/serban/empresarial](http://www.banamex.com.mx/serban/empresarial).
  - ✓ <http://bankos-unidos.com/banaamex>.
- Así mismo, a consecuencia del Spam se ha encontrado información fraudulenta, en nuestras direcciones de correo y medios electrónicos, de empresas y/o instituciones altamente confiables y reconocidas, motivo por el cual podemos ser víctimas de estos delitos.

Algunos de ellas son:

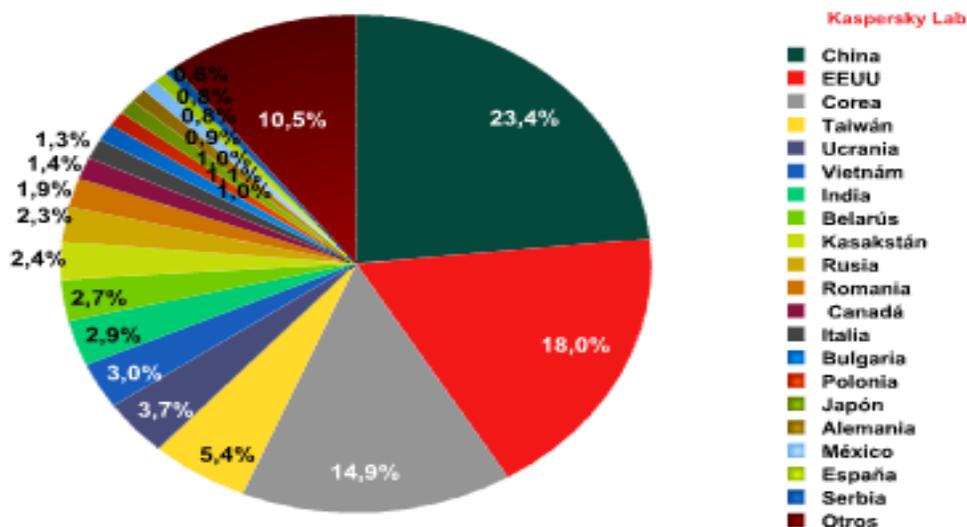
- ✓ **FEDEX.**
- ✓ **BURÓ DE CRÉDITO.**
- ✓ **PODER JUDICIAL DE LA FEDERACIÓN.**

La firma de seguridad McAfee señaló que en el primer trimestre del 2013 él envió de mensajes electrónicos no solicitados, marcó un incremento desfavorable a comparación del año pasado, ya que las cifras del 2012 eran de menos de un trillón y en el 2013 fueron de casi dos trillones en todo el mundo, cabe mencionar que nunca se habían registrado estos datos. Según el reporte de 2012, realizado por Norton Symantec, más de 14.8 millones de personas en México han sido víctimas de delitos informáticos en el último año, lo cual representó pérdidas por 2.2 billones de dólares.

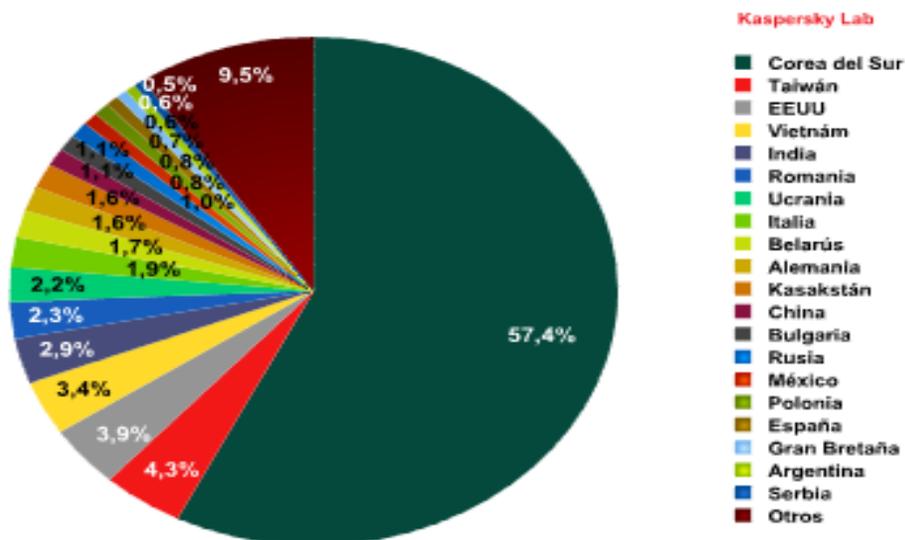
Las cifras obtenidas de 2013, muestran que nuestro país se encuentra en el top 20 de los principales países emisores de Spam, lamentablemente se está haciendo todo por permanecer e incluso aumentar su participación del mismo; los datos existentes son preocupantes ya que México entraba y salía de dicho listado, pero este año no se ha logrado salir, todo se debe al alto incremento de usuarios en los diversos medios electrónicos.

A continuación mostraremos dos graficas en las cuales observaremos claramente la información anterior<sup>137</sup>.

Fuentes de Spam en el mundo:



Fuentes de Spam en Europa, por país:



<sup>137</sup> Datos obtenidos en: <http://www.viruslist.com/sp/analysis?pubid=207271223>, consultada el 18 de julio de 2013 a las 19:00 horas.

### **5.3.1 Consideraciones que debe tomar el legislador para prevenir, proteger y sancionar el Spam.**

Es de vital importancia que el juzgador tenga en mente que diariamente, aparecen nuevas formas, temáticas del correo electrónico comercial no solicitado, que en la mayoría de las veces, puede ser con fines de índole comercial, y que este puede ser requerido o no por el destinatario, es menester aclarar que no sólo existe en el correo electrónico, sino lo pueden hacer a través de las distintas formas en que aparece el Spam, ya comentadas dentro de la investigación, incluyendo los mensajes de texto en los teléfonos móviles.

El legislador necesita una ley consistente, en donde se mencione, un concepto íntegro del correo electrónico no solicitado, así mismo como se le conoce cuando éste aparece en sus distintas formas, (scam, spim, phishing, etc.); para poder atacar de una manera más eficaz, dar soluciones a la problemática en cuestión, razón por la cual la mayoría de nosotros somos atacados constantemente.

El legislador a pesar de que trató, de regular al correo electrónico no solicitado, en La Ley Federal de Protección al Consumidor, la verdad no pudo combatir de lleno la problemática, considerando que ha dejado de lado la protección que atañe.

Es una problemática ya que no existe una ley al caso concreto, de aquí se derivan muchos más ilícitos penales, resultados o nuevas modalidades, a partir del correo electrónico comercial no solicitado

Nos hace referencia Miguel Ángel Davara Rodríguez, sobre ésta cuestión: “al no estar tipificado el “delito informático”, acudiremos atendiendo al principio de legalidad en materia penal indicador de la ley como creadora de delitos y penas al conocido principio <<*nullum crimen, nulla poena, sine lege*>> e indicaremos que

no habiendo ley que tipifique y, consecuentemente, indique la conducta delictiva.”<sup>138</sup>

La problemática por la cual se ve beneficiado el envío de Spam, es que su característica principal es de índole internacional y esto se debe a que el Internet no conoce fronteras territoriales, por ende uno puede enviar y recibir un correo electrónico de cualquier parte del mundo, pero el objetivo que no tenemos que olvidar es, utilizar esta gran herramienta que nos facilita la comunicación a distancia para beneficio y no por el contrario. Por este motivo varias naciones le han dado la importancia necesaria para poder combatirlo, pero sobretodo alertar a todos los perjudicados de que lo que está pasando, con el envío de correo electrónico comercial no solicitado, porque realmente se están cometiendo delitos que no podemos ignorar por completo.

La lucha no es fácil para enfrentar este problema, pero en verdad nos atañe a todos y por lo tanto debemos combatirlo juntos, la idea del proyecto es proporcionar los elementos necesarios con el fin de poder detectar esta situación, saber actuar a tiempo y no tener como resultado, el ser una víctima más del engaño.

Algunos países ya tienen una legislación para respaldarse, en caso de que se suscite algún delito, cuente con los medios adecuados para sancionar al individuo responsable por dichos actos.

Es de gran admiración que países desarrollados y subdesarrollados están tomando cartas en el asunto y han dado la iniciativa para sancionar este crimen. Algunos no lo abarcan del todo o sólo sancionan una parte, pero esto quiere decir que si preocupa a los grandes países la presencia del correo electrónico comercial no solicitado. Aunque hay que mencionar que donde se produce el mayor porcentaje de Spam es en EE.UU. y la ley que causo más revuelo es la

---

<sup>138</sup> Davara Rodríguez, Miguel Ángel, *Manual de derecho informático*, 4ª. ed., Madrid, España, Aranzadi, 2002, p. 336.

estadounidense conocida como CAN-SPAM, o ley de Control de agresiones de pornografía y marketing no solicitado.

Un aspecto muy importante que se debe destacar es, que no en todos los países, aunque resulte difícil de creer, se conoce esta problemática con el mismo término, no es tan relevante que se conozca de diferente forma o se le asigne un nombre diferente, pero si se debe saber cuál es el sinónimo correcto en cada país, para poder identificarlo. Lo que sí es preocupante es el hecho que lo que se considera ilegal, en un lugar del mundo en el otro se considera como legal, es por ello que se considere que al elaborar los Tratados así como la legislación mundial pertinente se tomen en cuenta:

- Identificación de problema, unificación de conceptos para lograr la prevención, encuadramiento del tipo pena y sanción.
- Colaboración de las autoridades correspondientes.
- Una cultura capaz de persuadir los inconvenientes, para el sector público como privado.
- Índice de SPAM en los diferentes países del mundo. Ejemplo claro se puedes apreciar, en el tercer trimestre del año 2012, el porcentaje de Spam en el tráfico de correo ha disminuido en un 2,8%, quedando en un promedio del 71,5%. A comparación del año 2011, donde el porcentaje del Spam en el tráfico de correo electrónico continuaba creciendo registrado un valor medio del 82,5%.
- Es importante hacer mención que nuestro País, ocupa el primer lugar de los países emisores, de información fraudulenta en cuanto a virus y malware.

Sin embargo a nivel mundial ciertos sectores, donde no había tanta reincidencia del correo no deseado, ha aumentado considerablemente como se puede apreciar en la tabla siguiente, que se encuentra en la página de Internet Kasperski Lab. <http://www.viruslist.com>:

<b>SECTOR MUNDIAL</b>	<b>PORCENTAJE (%) DE SPAM 2011</b>	<b>PORCENTAJE (%) DE SPAM 2012</b>
<b>Asia</b>	39, 22%	49, 50 %
<b>América del norte (EEUU+CANADÁ)</b>	2, 23%	27, 05%
<b>América latina</b>	22, 03%	7, 34%
<b>Europa occidental</b>	12, 17%	6, 86%
<b>Europa del este</b>	15, 39%	3, 64%
<b>Medio oriente</b>	4, 20%	3, 17%
<b>África</b>	3, 82%	2, 20%
<b>Australia + Oceanía</b>	0, 95%	0, 23%

Es importante destacar que países como Canadá, Japón, Estados Unidos e Inglaterra, poseen oficinas de gobierno específicas cuyas funciones van orientadas en la erradicación del Spam.

Desafortunadamente cifras actuales (año 2013) demuestran que nuestro país diariamente, sufre ataques cibernéticos cada vez más novedosos ocupando el primer lugar en toda América Latina, por lo que es primordial contar con una ley específica, que contemple dichas acciones para evitar pérdidas económicas, robo de identidad, daños en nuestras plataformas electrónicas.

Por lo anteriormente expuesto, propongo la creación de una ley especializada en la persecución de los mensajes electrónicos no solicitados, de índole comercial, político, religioso, contenido pornográfico, de piratería, educación, salud o de cualquier otro tipo, con el fin de que esta actividad sea castigada, es decir, existan disposiciones que realmente sancionen al que resulte responsable en elaborar dicha práctica y el delito no quede impune, al no existir un precepto legal que logre detener y así mismo no fomente dicha actividad en nuestro país, por lo tanto es necesario contar con una autoridad especial, la cual investigue, busque soluciones, encuentre al responsable e imponga sanciones a consecuencia del Spam.



## CONCLUSIONES.

Con base al camino realizado en nuestra investigación, podemos deducir lo siguiente:

**Primera.** El ser humano al constituirse en una sociedad, creó instrumentos que facilitaron las actividades cotidianas, claro ejemplo es la aparición del ábaco, gracias a este invento se revolucionaron las formas de poder organizarse creando instrumentos de trabajo para la comunicación y organización. Ante la necesidad de comunicarse con sus semejantes, se vió envuelto en crear herramientas para solventar esta misma, creando formas plasmadas en un papel, dando lugar a la imprenta, el periódico, y telégrafo, medios de comunicación como la radio y la televisión.

**Segunda.** La sociedad fue evolucionando y apareció nueva tecnología, que satisficieran las necesidades, por ello se logró la creación de instrumentos como la computadora y posteriormente el Internet. Con la aparición de Internet, pronto surgieron nuevas formas de comunicación que permitieron el intercambio y organización de la Información, dando lugar a la aparición del correo electrónico, actualmente se utiliza para el intercambio de información a distancia.

**Tercera.** El correo electrónico, representa una amenaza a nuestros equipos hoy día, pues con el surgimiento de él, también se derivó que las personas y empresas mandaran correos electrónicos a gran escala con contenido publicitario, teniendo como consecuencia la saturación del mismo. Ante el interés de ser un medio de intercambio de información a distancia, los sujetos aprovecharon para obtener un beneficio propio o en su caso perjudicar un equipo informático mediante el envío de información y/o datos maliciosos.

**Cuarta.** El Spam o correo electrónico comercial no solicitado es muy cambiante, es decir, aparecen nuevas modalidades con la tecnología y los individuos buscan formas de atacarlos, esto se debe a la falta de un precepto legal que se los impida.

**Quinta.** Debido a la problemática del Spam o correo electrónico no solicitado, países como los Estados Unidos de América (Can Spam Act); Unión Europea (ley directiva sobre la privacidad y las comunicaciones electrónicas); Australia (Spam Act); han creado legislaciones Anti-Spam para combatir este ilícito; brindando seguridad y protección de datos a sus usuarios. A la par se han realizado convenciones internacionales, teniendo como mayor propósito establecer un concepto internacional sobre el “Spam” y la unificación de una legislación penal nacional e internacional.

**Sexta.** Del análisis dogmático de la figura legal del Spam que se establece en la Ley Federal de Protección al Consumidor, se evidencia la falta de medidas de seguridad, de protección a los sujetos pasivos (personas físicas y moras), así como de las sanciones eficaces.

**Séptima.** Nuestro sistema jurídico necesita de manera urgente, reformas a nuestra legislación penal, para la contemplación de nuevos tipos penales, que hagan alusión a las formas de delinquir en Internet, es decir, los comúnmente llamados “delitos informáticos”, ya que si bien estas modalidades son innovadoras, los tipos legales aplicables en materia penal no lo son.

**Octava.** Es realmente necesario contar con una Ley Anti-Spam, que contemple sus modalidades del mismo: (verbigracia, el fraude), así como los medios comisivos que puedan surgir, por consiguiente, contemplar los sujetos especialistas que intervienen.

**Novena.** La dirección de correo debemos concebirla como una parte importante de nuestra personalidad, misma que permite identificar a la persona física o moral, es decir, no sólo es un nombre de dominio el cual sirve para acceder a las diferentes cuentas de correo que tengamos, sino debemos considerarlo como una forma de identidad, ante los demás.

**Décima.** Al observar los datos obtenidos respecto al porcentaje que existe de Spam tanto en México como en el mundo, estas cifras nos muestran que sigue presentándose este problema no sólo en el correo electrónico, también en distintas plataformas.

**Décima primera.** Los Gobiernos estatales deben concientizar a las personas a tomar medidas adecuadas para evitar el daño a nuestros equipos informáticos, así como el ser víctimas de delitos que se derivan a consecuencia del Spam, el que los legisladores creen una ley penal que sancione con medidas de seguridad, prisión y administrativas, así como la readaptación social a los sujetos especialistas en el ilícito. Por último el pensar en la existencia de una autoridad que se encargue de la persecución y sanción del Spam.

## **PROPUESTA**

### **CREACIÓN DE LEY ANTI-SPAM EN MATERÍA PENAL.**

Ante la presente era informática, Internet, las tecnologías y el correo electrónico, han surgido también nuevas formas maliciosas las cuales llegan a afectarnos a todos.

El legislador deberá de ser una persona que tenga conocimientos sobre las nuevas formas para delinquir en Internet, es decir, que sepa cómo se denominan las formas de ataque, contar con los conocimientos y tecnicismos a fines al tema.

Firmar Convenios con los países que, ya cuentan con una legislación en la materia, así como, dar seguimiento a los Convenios Internacionales en materia Informática, se logre una cooperación bilateral y brindar los elementos necesarios tendientes a erradicarlo.

Existen otras formas de regular el Spam, una de ellas es la inclusión de un capítulo, en el Código Penal Federal; otra, incluir una extensión a los artículos de la Ley Federal de Protección al Consumidor, en los que se relacionen con el Código Penal Federal Título IX, Capítulo II Acceso ilícito a sistemas y equipos de informática, para que existan medidas de seguridad acorde al ilícito, y que no sólo se apliquen medidas administrativas; o bien crear una Ley especial Anti-Spam.

La anterior inclusión en materia penal debe considerar la protección informática de datos personales, tendientes al correo electrónico no solicitado.

La dirección de correo electrónico se debe concebir como un elemento de la personalidad. El objetivo principal es que se cree una Ley Federal Anti-Spam que imponga penas y sanciones a los responsables de dichos actos.

## **PROPUESTA DE LEY FEDERAL ANTI-SPAM EN MATERIA PENAL.**

### **Artículo 1º.- Objeto de la Ley.**

La presente Ley tiene por objeto regular el envío de mensajes electrónicos no solicitados o Spam, sean o no de carácter publicitario, proteger a las personas y empresas que sufren un daño, como consecuencia del Spam, reparar el daño por recibir información o contenido malicioso, que daña sus redes informáticas, equipos de cómputo e información valiosa almacenada en sus bases de datos, las cuales representan enormes pérdidas.

### **Artículo 2º.- Definiciones.**

a) Correo electrónico:

Es aquel servicio de Internet que permite a los usuarios, enviar y recibir información de forma instantánea.

b) INPES: Instituto Nacional para la prevención de los Mensajes no Solicitados, para efectos de esta ley se considera la autoridad encargada en la persecución del delito de Spam.

c) Mensaje electrónico:

Es aquel mensaje que se transmite a través de la red entre computadoras o cualquier equipo de tecnología existente.

d) Mensaje electrónico comercial:

Todos los mensajes electrónicos son considerados de índole comercial, cuando el contenido de los mismos haga referencia para promocionar bienes y servicios.

e) Mensaje electrónico no solicitado o Spam:

Lo consideramos como aquella información que no hemos solicitado, pero que se recibe por cualquier medio electrónico e informático, no sólo de carácter publicitario, sino de cualquier índole. Con el objeto de engañarnos al ser dirigidos a sitios web falsos, para la obtención de datos confidenciales para terceros, con ánimos de lucro.

f) Phishing:

Fraude tradicionalmente cometido a través de Internet, que pretende conseguir datos confidenciales de usuarios, robando la identidad de los mismos, utilizando las contraseñas o claves de acceso de las cuentas bancarias, para sí o un tercero con ánimos de lucro.

**Artículo 3.- Clases de Spam.**

Para efectos de esta Ley, se consideran mensajes electrónicos no solicitados, no sólo los de carácter comercial, sino aquellos que contengan información de índole político, religioso, contenido pornográfico, de piratería, educación, salud o de cualquier otro tipo.

**Artículo 4.- Sujetos que intervienen.**

Se consideran sujetos que intervienen en envío de Spam:

- a) Remitente: es aquel individuo que redacta y envía el correo o mensaje electrónico no solicitado a uno o varios destinatarios, a fin de hacer de su conocimiento el contenido a los destinatarios.
- b) Servidor: es aquella plataforma, que sirve como enlace entre el remitente y el destinatario, para enviar y recibir la información mencionada.

c) Destinatario: son las personas físicas o morales, propietarios, titulares de la dirección de correo electrónico o cualquier otro medio electrónico que permita el envío de mensajería informática.

**Artículo 5.-** Queda prohibido crear, enviar, dañar, modificar, copiar, utilizar información, mediante mensajes electrónicos, textos, imágenes, publicidad o algún otro medio, que cause daño a un sistema informático.

**Artículo 6.-** Se prohíbe la distribución de mensajes electrónicos, cuyo contenido sea información falsa, misma que puede inducir a error a los destinatarios.

**Artículo 7.-** Se prohíbe la distribución de direcciones electrónicas, números telefónicos y toda información de carácter personal, a empresas de marketing, que tengan ánimo de lucro para sí o un tercero. Es equiparable a los delitos contenidos en los artículos 17, 18, 18 bis, 32 de la Ley Federal de Protección al Consumidor.

**Artículo 8.-** Es equiparable al delito de Acceso ilícito a sistemas y equipos informáticos, el cual está regulado en el artículo 211 bis del Código Penal Federal.

**Artículo 9.-** Es equiparable al delito de Fraude, el cual es regulado en el artículo 386 del Código Penal Federal.

**Artículo 10.-** Es equiparable al delito de Falsificación, el cual está regulado en el artículo 243 del Código Penal Federal.

**Artículo 11.-** Queda prohibida la utilización de los mensajes electrónicos e informáticos, para la distribución de virus (malware, spyware), para dañar, eliminar, alterar información e infiltrarse en los equipos electrónicos.

**Artículo 12.-** Se prohíbe la utilización de programas y/o aplicaciones desarrolladas, cuya finalidad sea, para la recolección masiva de direcciones electrónicas a través de Internet o algún otro mecanismo para obtener información del destinatario, en las diversas tecnologías.

**Artículo 13.-** Se considera ilegal la utilización de las estafas electrónicas como el phishing, etc., cuyo fin es engañar al destinatario en el momento, en que este se encuentra en una página en Internet supuestamente autentica, cuya finalidad es aprovecharse de la situación para obtener datos personales y confidenciales.

**Artículo 14.-** En caso de obtener datos y/o información confidencial de los destinatarios, se prohíbe utilizar estos mismos, para algún beneficio del o las personas responsables de los mensajes electrónicos.

**Artículo 15.-** Al recibir los mensajes electrónicos no solicitados, estos deben de expresar claramente que contienen publicidad o se trata de Spam, así como incluir información clara y autentica, la cual sirva para identificar quien nos envía estos mensajes.

**Artículo 16.-** El sujeto activo del Spam, pueden ser personas físicas o morales, es decir, las empresas a través de su representante legal, que con tal de darse a conocer en el mercado, realizan esta actividad enviando publicidad, la cual puede ser lícita para ellos, sin embargo para los usuarios es calificada como Spam.

**Artículo 17.-** Se considera lícita la información cuando el usuario contrate con la empresa algún bien o servicio, mismo que es considerado por la empresa como destinatario final; sin perjuicio de lo anterior, el destinatario final tiene la facultad para solicitar con posterioridad al contrato, que no se les envíe más información al respecto.

**Artículo 18.-** De lo establecido en el anterior artículo, cuando el usuario expresa que no desea recibir más información y la empresa haga caso omiso, será acreedora a la sanción administrativa establecida en la Ley Federal de Protección al Consumidor, sin perjuicio de la sanción penal establecida en esta Ley.

**Artículo 19.- Sanción pecuniaria.**

El destinatario, que resulte afectado como consecuencia de los mensajes electrónicos no solicitados, podrá ejercer acción penal en contra del remitente, los cuales pueden ser empresas, usuarios o quien resulte responsable.

**Artículo 20.- Reparación del daño.**

Con independencia a lo establecido en el anterior artículo, el responsable se hará cargo de la reparación del daño ocasionado o prestará servicio comunitario en alguna dependencia de gobierno bajo la supervisión del Instituto Nacional para la Prevención de los Mensajes Electrónicos no Solicitados.

**Artículo 21.-** No se aplicaran las penas previstas en esta Ley, si se comprueba que no son responsables, por los daños ocasionados en los equipos informáticos y/o electrónicos por el mal manejo de los mismos.

**Artículo 22.-** La autoridad competente en la persecución de este delito, coadyuvante del Ministerio Público y la Procuraduría Federal del Consumidor, será el Instituto Nacional para la Prevención de los Mensajes Electrónicos no Solicitados, (INPES).

**Artículo 23.-** Para los supuestos contenidos en esta ley se impondrán de 2 a 5 años de prisión; se incrementara la pena en una mitad, cuando dichos actos sean cometidos por servidores públicos o personal, directores, representantes, entre otros según sea el caso, que tenga por objeto el ánimo de lucro para sí o para un tercero, y al monto que se establece en la Ley de protección al consumidor, así mismo serán acreedores a la suspensión o remoción del cargo.

**Artículo 24.-** Salvo indicación en contrario, la presente Ley se extiende a los actos, omisiones, asuntos y cosas fuera de México.

## BIBLIOGRAFÍA.

1. AGUILAR LÓPEZ, Miguel Ángel, *El Delito y la Responsabilidad Penal. Teoría, Jurisprudencia y Práctica*, 4ª. ed., México, Porrúa, 2008.
2. AMUCHATEGUI REQUENA, Irma Griselda, *Derecho Penal*, 3ª. ed., México, Oxford, 2005.
3. ANDREU GÓMEZ, Joaquín. *Servicios en red. Informáticos y comunicaciones*, España, Editex, 2010.
4. ARILLA BAS, Fernando, *Derecho penal. Parte general*, México, Porrúa, 2001.
5. AZAOLA CALDERÓN, Luis, *Delitos Informáticos y Derecho Penal*, México, Ubijus, 2010.
6. CÁMPOLI, Gabriel Andrés, *Delitos Informáticos en la Legislación Mexicana*, México, Instituto Nacional de Ciencias Penales. INACIPE, 2005.
7. CÁMPOLI, Gabriel Andrés, *Principios de Derecho Penal Informático*, México, Ángel editor, Instituto Nacional de Ciencias Penales. INACIPE, 2004.
8. CARRANCÁ Y TRUJILLO, Raúl y Carrancá y Rivas, Raúl, *Derecho penal mexicano. Parte general*, 22ª. ed., México, Porrúa, 2004.
9. CASTELLANOS HERNÁNDEZ, Eduardo, *et al.*, *Temas de Derecho Informático*, México, Orden jurídico nacional, Secretaria de Gobernación, SEGOB, 2006.
10. CASTELLANOS TENA, Fernando, *Lineamientos elementales de Derecho Penal*, 44ª. ed., México, Porrúa, 2003.
11. CHACÓN, ALVARADO, Lucía, *Automatización de la Biblioteca*, Costa Rica, Universidad Estatal a distancia, 2002.
12. DAVARA RODRÍGUEZ, Miguel Ángel, *Manual de Delitos Informáticos*, 4ª. ed., España, Aranzadí/ A thonsan company, 2002.
13. DAZA GÓMEZ, Carlos, *Teoría general del delito sistema finalista y funcionalista*, 5ª. ed., México, Flores Editor y Distribuidor S.A de C.V, 2006.
14. DÍAZ ARANDA, Enrique, *Derecho penal. Parte general*, 3ª. ed., México, Porrúa, 2003.

15. F. KUHLMANN, A. Alonso, *Información y telecomunicaciones*. México, Fondo de Cultura Económica, 1996.
16. GUERRERO CAÑONGO, Juan Antonio, *Los mejores secretos para ganar dinero*, México, Panorama Editorial, S. A. de C. V., 2007.
17. JIMENEZ MARTINEZ, Javier, *Elementos del Derecho Penal Mexicano*, México, Porrúa, 2006.
18. JÍMENEZ MÁRTINEZ, Javier, *Introducción a la teoría general del delito*, 2ª. ed., México, Ángel editor, 2005.
19. JIMÉNEZ ZAMORA, Arturo, *Manual de Derecho Penal*, México, Ángel Editor, 2000.
20. MESSÍA DE LA CERDA BALLESTEROS, Jesús Alberto, *La protección de datos de carácter personal en las telecomunicaciones*, España, Dykinson, S. L., 2004.
21. MEZGER, EDMUND, *Derecho Penal*, 2ª. ed., México, Cárdenas Editor y Distribuidor, 1990.
22. MOLINA SALGADO, Jesús Antonio, *Breviarios Jurídicos en el Derecho de la Propiedad Industrial*, México, Porrúa, 2003.
23. MUÑOZ TORRES, Ivonne Valeria, *Delitos Informáticos. Diez años después*, México, Ubijus, 2009.
24. NAVARRO ISLAS, Jorge, *Tecnologías de información y de las comunicaciones y comercio electrónico: Aspectos legales*, México, AMIPCI, 2008.
25. PALAZZI, Pablo Andrés, *Delitos Informáticos*, 3ª. ed., Argentina, Ad-Hoc, 2000.
26. PARDINI, Aníbal Alejandro, *Derecho de Internet*, Argentina, La Roca, 2003.
27. PEREA QUINTANA, Claudia Mireya, *Poder Judicial del Estado de Chihuahua*, México, año V, número 7, Supremo Tribunal de Justicia, 1999.
28. SANCHEZ DEL CATILLO, Vilma, *Publicidad en Internet régimen jurídico de las comunicaciones electrónicas*, España, La Ley, Grupo Wolters Kluwer, 2007.

29. RIBAS ALEJANDRO, Francisco Javier, *Aspectos Jurídicos del comercio electrónico en Internet*, España, Aranzadi, 1999.
30. TÉLLEZ VALDÉS, Julio, *Derecho Informático*, 4<sup>a</sup>. ed., México, Mc Graw Hill, 2008.
31. TÓMAS AZPILCUETA, Hermilio, *Derecho Informático*, Argentina, Abeledo-Perrot, 1987.
32. UROSA RAMIREZ, Gerardo Armando, *Teoría de la Ley Penal y del Delito. (Legislación, Doctrina, Jurisprudencia y Casos Penales)*, México, Porrúa, 2006.
33. VERGARA TEJADA, José Moisés, *Manual de Derecho Penal. Parte General*, México, Ángel Editor, 2002.

### **Fuentes Legislativas.**

#### **MÉXICO.**

34. Constitución Política de los Estados Unidos Mexicanos, 27<sup>a</sup>. ed., México, Ediciones Fiscales Isef, 2013.
35. Código Penal Federal, 12<sup>a</sup>. ed., México, Sista, 2013.
36. Ley Federal de Protección al Consumidor, disponible en: [http://www.profeco.gob.mx/juridico/pdf/l\\_lfpc\\_ultimo\\_camDip.pdf](http://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_camDip.pdf), consultada el 01 septiembre de 2011 a las 10:30 horas.
37. Ley Federal del Trabajo, disponible en: [http://www.stps.gob.mx/bp/micrositios/reforma\\_laboral/archivos/Noviembre.%20Ley%20Federal%20del%20Trabajo%20Actualizada.pdf](http://www.stps.gob.mx/bp/micrositios/reforma_laboral/archivos/Noviembre.%20Ley%20Federal%20del%20Trabajo%20Actualizada.pdf), Consultada el 19 de julio de 2012 a las 17:00 horas.
38. Ley de Protección de Datos Personales en Posesión de los Particulares, vigente 2013, disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>, consultada el 13 de agosto de 2011 a las 13:00 horas.

39. Ley de la Propiedad Industrial, vigente 2013, disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/50.pdf>, consultada el 23 de agosto de 2012 a las 14:30 horas.

### **Fuentes de legislación internacional:**

#### **ARGENTINA.**

40. Ley de Protección de Datos Personales 2000, disponible en: <http://www.red.org.ar/ley.htm>, consultada el 11 de junio de 2011 a las 11:00 horas.

#### **AUSTRALIA.**

41. Spam Act 2003 (texto extraído, traducido y adaptado. Rodríguez García, Eric Ernesto), disponible en: <http://www.comlaw.gov.au/Details/C2013C00021>, consultada el 17 de julio de 2011 a las 11:00 horas.

#### **ESPAÑA.**

42. Ley de Servicios de la Sociedad de la Información y Comercio Electrónico 2002, disponible en: [http://noticias.juridicas.com/base\\_datos/Admin/l34-2002.t1.html#a1](http://noticias.juridicas.com/base_datos/Admin/l34-2002.t1.html#a1), consultada el 02 de mayo de 2011 a las 13:00 horas.

#### **ESTADOS UNIDOS.**

43. Can Spam Act 2003. (texto extraído, traducido y adaptado. Rodríguez García, Eric Ernesto), disponible en: <http://www.spamlaws.com/federal/108s877.shtml>, consultada el 23 de abril de 2011 a las 12:30 horas.

44. Acta Federal de Abuso Computacional, disponible en: <http://legal.web.aol.com/resources/legislation/ecpa.html>, consultada el 26 de abril de 2011 a las 13:30 horas.
45. Legislación acerca del uso de internet, disponible en: [http://www.inf.utfsm.cl/~lhevia/asignaturas/infoysoc/topicos/Etica/8\\_legislacion\\_acerca\\_uso\\_internet.pdf](http://www.inf.utfsm.cl/~lhevia/asignaturas/infoysoc/topicos/Etica/8_legislacion_acerca_uso_internet.pdf), consultada el 28 de abril de 2011 a las 15:00 horas.

## **UNIÓN EUROPEA.**

46. LEY DIRECTIVA SOBRE LA PRIVACIDAD Y LAS COMUNICACIONES ELECTRÓNICAS 2002. (texto extraído, traducido y adaptado. Rodríguez García, Eric Ernesto), disponible en: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:es:NOT>, consultada el 31 de mayo de 2011 a las 14:00 horas.

### **Fuentes electrónicas:**

47. [www.alegsa.com.ar](http://www.alegsa.com.ar)
48. [www.apec.org](http://www.apec.org)
49. [www.cnnexpansion.com](http://www.cnnexpansion.com)
50. [www.eset.la.com](http://www.eset.la.com)
51. [www.itu.int/pages/default.aspx](http://www.itu.int/pages/default.aspx)
52. [www.itu.int/wisis/index.es.html](http://www.itu.int/wisis/index.es.html)
53. [www.interbusca.com](http://www.interbusca.com)
54. [www.oecd-antispam.org](http://www.oecd-antispam.org)
55. [www.protecciondedatos.com.ar](http://www.protecciondedatos.com.ar)
56. [www.rae.es](http://www.rae.es)
57. [www.wikipedia.com](http://www.wikipedia.com)