TESIS PARA OPTAR AL GRADO DE MAGÍSTER EN DERECHO INFORMÁTICO Y DE LAS TELECOMUNICACIONES.

Spam y su regulación en Chile. ¿Cómo obtener la Protección Jurídica de la intimidad de las personas, sin afectar el desarrollo legítimo de una actividad económica?

Candidato: **Jorge Salvador Dávila Arancibia**

Profesor Guía: **Lorena Donoso Abarca**

Facultad de Derecho

Universidad de Chile

INDICE

INTRODUCCIÓN

Sin duda para nadie el SPAM significa a esta altura de la vida una palabra desconocida, en que hemos aceptado la intromisión casi silenciosa en nuestras vidas del Internet y sus formas de comunicación masiva.

Lo que si no podemos negar, es que el SPAM, se ha transformado hoy día en un actor importante de esta forma de vida de miles de personas, afectando directamente, tanto a los usuarios, operadores y otros actores, como pueden ser las empresas que legítimamente se dediquen al telemarketing.

A su vez dichas disquisiciones técnicas, son estrictamente necesarias a la hora de estudiar las distintas leyes, prácticas de buenas costumbres y propuestas para legislar adecuadamente; de manera que se pueda establecer adecuadamente las medidas técnicas-legislativas pertinentes.

Por ello para el adecuado desarrollo de este trabajo, será necesario dedicarnos algunas páginas a un capítulo eminentemente de carácter técnico, cuyo principal objetivo será el ser una base al desarrollo del tema central de este estudio, toda vez que las implicancias jurídicas que el SPAM puede presentar, tienen su origen tanto en el sistema empleado por los operadores para otorgar el servicio y la forma en que los usuarios de casillas de correo electrónico utilizan el servicio, que permite que terceros abusen tanto de las deficiencias del sistema, como la llamada “opacidad de la red”, término que se convirtió en un verdadero paradigma hace algunos años, y que hoy a mi parecer ya es un recuerdo del pasado.

Realizadas las aclaraciones técnicas, continuaremos, analizando el SPAM

en cuanto tal, y otras figuras anexas, para poder centrarnos en su estudio jurídico y problemáticas reales que trae aparejadas.

Nos adentraremos en la regulación que se le ha dado a este problema en otras legislaciones, en especial recurriremos a la experiencia de la Unión Europea, la norteamericana y de algunos países latinoamericanos, para finalmente dejarnos caer en la experiencia nacional, poca por decir lo menos, en que a través de distintos proyectos de ley, hoy día todos archivados, se ha llegado sólo a un par de normas incluidas en la ley de Defensa del consumidor, cuya efectividad ha sido prácticamente nula.

Hecho lo anterior, haremos lo posible por desentrañar otros problemas propios del SPAM, viendo quienes son responsables, problemas aparentemente insalvables como la extraterritorialidad, etc, para de una u otra manera ser capaces de realizar un aporte a nuestra realidad, entregando un esquema macro de lo que debiera considerar una eventual ley para nuestro país, que sea capaz de regular este problema, sin afectar derechos validos de terceros actores.

I.- CUESTIONES TECNICAS PREVIAS

1º.- Conceptos fundamentales

Con el fin de abordar correctamente el servicio de correo electrónico, es imprescindible establecer los siguientes conceptos previos, los cuales se utilizaran permanentemente a lo largo de este trabajo.

a.- **Usuario:** Persona natural o jurídica, que usa un servicio de acceso o de correo electrónico.

b.- **Equipos:** Todo dispositivo que permita la comunicación y la utilización de servicios en la Internet, tales como pueden ser computadoras, agendas electrónicas, celulares y otros equipos de tercera generación.

c.- **Red:** Grupo de equipos conectados entre sí.

d.- **Internet:** Grupo de redes conectadas y que permiten que los datos viajen desde un punto a otro.

e.- **Aplicación:** Cualquier programa que corra en un sistema operativo y que haga una función específica para un usuario. Por ejemplo, procesadores de palabras, bases de datos, agendas electrónicas, etc[1]

f.- **Conexión:** Trayectoria que seguirán los datos en la red para establecer una comunicación entre dos equipos.

[1] Glosario de informática e Internet [en línea].Panamá. [Fecha de consulta: 11 diciembre 2008] Actualización permanente. Disponible en: http://www.panamacom.com/glosario/letra-a.html

g.- **Proveedor de Servicio Internet (en inglés, ISP - Internet Service Provider):** Empresa que provee la conexión de computadoras a Internet, ya sea por líneas dedicadas broadband o dial-up.[2]

h.- **Proveedor de Servicio de Correo (en inglés, MSP - Mail Service Provider):** Es una organización que se encuentra previamente conectada a la Internet y que provee de servicio de correo a sus clientes. Hay que dejar establecido desde ya, un Proveedor de Servicio de Internet no necesariamente requiere ser proveedor de servicio de correo y viceversa. No obstante, un ISP por lo general provee de servicio de correo a sus clientes.

i.- Cuenta - Cuenta de acceso: Parámetros que se asignan a un usuario de manera de poder ser identificado y autorizado para poder ingresar a algún servicio de la red (conexión, correo, chat y otros)

j**.- Protocolo:** Es el diseño que especifica los detalles sobre la manera en que se relacionan los equipos, incluyendo el formato de los mensajes que intercambian y el manejo de los errores. Es el lenguaje con el cual hablan los dispositivos entre sí.

k.- **Internet Protocol - IP (en español, "Protocolo Internet**") Este protocolo define las reglas necesarias para permitir el tránsito e intercambio de datos a través de las interconexiones entre las distintas redes disponibles o dentro de la red global de Internet.

l.- **Dirección o Número IP:** Numeración especial que identifica a un equipo dentro de una red. Cumple la misma función que un número "de teléfono" dentro de la red de telefonía. Una conexión requiere de la asignación de una dirección IP, ya que ésta es necesaria para intercambiar

[2] Glosario de informática e Internet [en línea].Panamá. [Fecha de consulta: 11 diciembre 2008] Actualización permanente. Disponible en: http://www.panamacom.com/glosario/letra-i.html

datos entre equipos conectados a la red.

m.- **Dirección IP Pública:** En el caso de las direcciones IP Públicas, son únicas y conocidas dentro de Internet, por lo tanto son alcanzables desde cualquier punto de ésta y no pueden ser utilizadas por más de un equipo al mismo tiempo. Son similares a los números de teléfono que utilizamos normalmente.

n.- **Dirección IP Privada:** En el caso de las IP Privadas, éstas son alcanzables sólo desde un segmento específico, y pueden ser utilizadas por varios equipos que estén en diferentes redes al mismo tiempo, siempre y cuando estas redes estén directamente conectadas (Por ejemplo: Al interior de una empresa) En el caso que dos o más redes privadas estén interconectadas entre sí, es necesario realizar un enmascaramiento de las direcciones de IP de origen y de destino. Esto se conoce como **NAT** (Network Address Translation, "traducción de direcciones de red") Este funcionamiento es similar a los "anexos" dentro de una central telefónica, los cuales son como las IP Privadas dentro de la red. Para conectarse a la red telefónica, un anexo disca hacia afuera, pero al receptor le aparece el número de teléfono de la central en vez de aparecer el número de anexo, por lo tanto hay una "traslación" del nombre. Este proceso es similar al NAT que se realiza en el caso que un cliente con IP Privada necesite conectarse con una red Pública o con otra red privada.

ñ.- **Dirección de IP Dinámica:** Es la dirección IP pública que se otorga automáticamente al cliente en el momento de conexión. Esta dirección IP se mantendrá vigente hasta que se produzca una desconexión por parte del cliente o del proveedor. Esta dirección IP puede ser distinta en cada conexión, y será definida por el proveedor de servicio Internet de acuerdo a la disponibilidad de direcciones IP públicas que éste tenga en el momento

específico en el cual se realiza la conexión.

o.- **Dirección de IP Fija:** Es la dirección IP pública que se asigna a un cliente en su proceso de conexión. Esta dirección IP pública es la misma en cada conexión. Es asignada por el proveedor de servicio Internet a un cliente en particular, lo que significa que este cliente siempre podrá ser identificado por esa dirección IP.

p.- **Emisor:** Es la persona que envía un mensaje por correo electrónico.

q.- **Originador:** Es la persona cuya identificación está expresada en el remitente del mensaje de Correo Electrónico (símil a un sobre en el Correo tradicional), no necesariamente es la persona que envía.

r.- **Receptor:** Es la persona que recibe el mensaje de Correo Electrónico.

s.-**Destinatario:** Representa la persona a quien está dirigida la comunicación electrónica y que es indicada como remitente del mensaje electrónico (símil a un sobre en el Correo tradicional), no necesariamente es la persona que recibe.

t.- **Mensaje:** Es el equivalente a la carta que se incluye dentro de un sobre, y que es donde se contiene la comunicación que se pretende enviar; la cual puede o no contener adjuntos.

u.- **Adjuntos:** Representa los adicionales que se pueden incorporar dentro de un mensaje electrónico y que forman parte del contenido del mensaje, como por ejemplo. Fotos, informes, u otras componentes que podrían incluso ser ejecutadas.

v.- **Buzón - casillas:** Representa el lugar de almacenamiento donde se

aloja el correo y donde sólo el dueño tiene la posibilidad de verlos y borrarlos. Una persona puede poseer muchas cuentas de correo y por ende varias casillas.

w.- **Dominio de correo:** Representa el equipo que administra la casilla de correo de un cliente.

x.- **Dirección de correo:** Es la dirección postal de quien envía o recibe un correo. En el caso del correo electrónico, esta dirección se compone de dos partes; la primera identifica el buzón del usuario y la segunda el equipo en el que se ubica el buzón.
Ejemplo: fulano@gmail.com en donde:
fulano → identifica el buzón del usuario.
Gmail.com → identifica el servidor en el que se ubica el buzón.

Hay que hacer presente que al igual que en un sistema tradicional de correo, tanto el nombre de usuario como el dominio de correo pueden ser alterados o simplemente no existir. Este comentario merece especial atención, ya que los emisores de SPAM suelen alterar estos parámetros con el fin de dificultar su detección, para ello se abastecen de programas que automáticamente van variando estos atributos. Una acción frecuente que también usan es la de hacerse pasar por remitente válido, es decir, "Robo de Identidad".

y.- **Cuenta de correo:** Es la identificación, usuario y contraseña, para usar el servicio de correo. En un sistema tradicional corresponde a la llave física que abre un buzón o casilla.

z.- **Correo electrónico (en inglés, e-mail):** Es el nombre del servicio que permite que un mensaje electrónico se traslade desde un origen a un

destino. También es utilizada para identificar la dirección a la cual se deben enviar los correos.

a1.- **Servidor de correo:** Representa la oficina postal que identifica al destinatario como su cliente. El servidor recibe el correo y lo deposita en la casilla hasta que sea requerida por su dueño (destinatario)

a2.- **SMTP (Simple Mail Transfer Protocol) o Protocolo de Transferencia de Correo Simple:** es el lenguaje o protocolo utilizado para el transporte de correo.

a3.- **Sistema Opt-out o de exclusión:** Sistema de envío de correo electrónico, en virtud del cual el destinatario puede rechazar toda correspondencia futura de este tipo. El primer mensaje no deseado se aceptará siempre y permanecerá así hasta que el destinatario modifique la opción. En virtud de ello, el emisor debe incluir siempre las instrucciones específicas que permitan al destinatario solicitar su remoción de manera simple y gratuita.

a4.- **Sistema Opt-in o de inclusión:** Sistema de envío de correo electrónico, en virtud del cual sin la autorización previa de los destinatarios no pueden ser enviados. La autorización debe concederse explícitamente y el emisor puede obtenerla por cualquier medio.

2º.- Descripción de un sistema de correo electrónico.

Previo a definir que entendemos por Servicio de Correo electrónico, hay que decir que dicho servicio forma parte del llamado sistema de Correo Electrónico, el cual se conforma además por el Servicio de Conexión o Acceso.

Al respecto debemos señalar que el sistema de correo electrónico se compone por una parte del servicio de Conexión, llamado también Servicio de Acceso, y del servicio de Correo Electrónico.

En Cuanto al servicio de Acceso podemos decir en términos simples que es "aquella prestación de conexión que un ISP (que puede ser MSP o no) conectado a la red provee a un usuario del servicio de correo electrónico". Este usuario de servicio de correo puede ser de dos clases, el primero, monousuario que corresponde a aquel que sólo conecta un equipo al ISP y el segundo, multiusuario, que es aquel que a través de un equipo conectado al ISP existe una red interna que hace uso de esta conexión.

En el caso de una conexión de un monousuario, su aplicación de conexión envía al ISP los datos de su cuenta de acceso (usuario y contraseña), el ISP una vez que chequea que ésta información sea correcta, lo autoriza y le retorna al equipo del cliente una dirección IP pública (conocida en Internet); siguiendo Internet autónomamente, red que reconoce los datos de ese equipo por la dirección IP (fija o dinámica según sea el caso) que le fue asignada.

Tratándose de un cliente multiusuario, generalmente se debe disponer de un equipo que permita la conexión y además sea capaz de pasar los datos, de los computadores que conforman la red, al ISP. Al igual que en el caso anterior este equipo, que solicita acceso al ISP, requiere autentificarse; para ello envía al ISP los datos de su cuenta de acceso (usuario y contraseña), el ISP una vez que chequea que ésta información sea correcta, lo autoriza y le retorna al equipo del cliente una dirección IP pública (conocida en Internet) En este escenario hay que distinguir dos posibles situaciones.

La primera, Internet no sabe que detrás de ese equipo de conexión existen otros computadores, cree que es sólo uno, pues éste funciona como intermediario entre la Internet y la red interna del cliente, la cual usa direcciones IP privadas y el equipo que esta conectado al ISP usa una dirección IP pública.

La segunda situación, es aquella en que cada uno de estos equipos de la red del cliente les sea asignado una dirección IP pública, operando similar al del usuario monousuario.

Habiendo establecido el servicio de acceso, podemos acercarnos ya al servicio de Correo Electrónico.

Sin duda, la mejor manera de entender el concepto de correo electrónico es establecer una analogía con el tradicional servicio de correo, con el cual sólo se diferencia por el hecho de que la materialidad de la carta, es reemplazada por un dispositivo automático que envía el mensaje electrónicamente.

El usuario para enviar un correo electrónico, debe ingresar los datos de su cuenta, es decir nombre de usuario y contraseña, la cual una vez ingresada es enviada al servidor de correo para ser validada y en caso de ser correcta, se le autoriza a ingresar al servicio. De ahí en adelante queda establecida una comunicación entre la aplicación que utilice el cliente para leer correo (también llamado cliente de correo) y el servidor de correo.

Hay que hacer presente que en un proceso de correo, un cliente es considerado emisor y receptor a la vez, en el momento que envía y recibe correos respectivamente.

El cuanto al acceso al servicio de correo electrónico, este normalmente se realiza a través de la utilización de aplicaciones especialmente diseñadas para esto; las cuales se caracterizan por ser capaces de conversar con los servidores de correo de forma tal de realizar intercambio de correos, es decir, enviar o recibir. Los medios de acceso más usados son "webmail" y "clientes de correo".

En cuanto al llamado webmail, es el acceso al servicio de correo electrónico, mediante la utilización de un navegador web, (Internet Explorer, Netscape, Mozilla, Opera, etc). A través de éste se indica la dirección web en donde se aloja el servicio de correo que el usuario requiere acceder. Las características y funcionalidades que contenga este servicio de correo son definidas por el MSP.

Por su parte el "Cliente de correo", concepto que no debe confundirse con el usuario, o sea, la persona emisor/receptor que accede a su correo; es el nombre que se le asigna a la aplicación o software que se instala en el equipo de un usuario (emisor/receptor) y que se comunica con el servidor de correo para enviar y/o recibir, como ocurre con los conocidos softwares Outlook Express y Eudora, entre otros.

3º.- Los Correos masivos y su tratamiento por los ISP

En este numeral analizaremos los correos masivos, que pueden tener su origen en Chile como en el extranjero y cuyo destino es un Proveedor de Servicio de Correo Nacional.

En primer lugar debemos señalar que entenderemos por "Correo masivo",

a toda emisión masiva de correo electrónico originada por un único emisor, la cual no discrimina el contenido del mensaje, es decir, puede ser cualquier tipo de correo entre ellos el SPAM.

Estos correos, sean o no SPAM, para la mayoría de los usuarios, así como para los ISP y para los MSP, son un problema. En atención a ello, y a fin de evitarlos o tratar de disminuirlos a su máxima expresión, los MSP, aplican controles sobre el proceso de todo correo electrónico.
Entre las medidas mas comunes de utilización por los MSP, se encuentran las siguientes:

- **Listas Negras:** El sistema de listas negras, se basa en directorios elaborados por los distintos MSP e ISP, tanto nacionales como internacionales. Estas listas son conocidas y reconocidas por los MSP, se construye con los números IP que han sido identificados como emisores de correo masivo. Las nacionales son construidas y compartidas por acuerdo de los ISP; requieren procesos de coordinación y comunicación para accederlas y operarlas; y su financiamiento es compartido por aquellos que hacen uso de ellas. En cuanto a las internacionales, son manejadas como servicio a nivel Internacional y son utilizadas por múltiples MSP, en algunos casos previo pago de una suscripción.

- **SMTP autentificado de salida:** El que el SMTP sea autentificado significa que se realiza una autentificación y verificación del nombre de usuario y contraseña de quien intenta realizar el envío, de manera de elevar los niveles de seguridad y eficacia del servicio de correo electrónico y con el objetivo de minimizar la posibilidad que una cuenta sea utilizada sin autorización para el envío de correo.

- **Control de destinatarios por mensajes**: Esta acción impide que los clientes hagan envío de correo a una cantidad de destinos superior a un máximo que se haya establecido en el sistema.

- **Control del tamaño de un correo:** Esta acción impide que los clientes hagan envío de correo de tamaño superior a un máximo que se haya establecido en el sistema.

- **Control de Dominio y Usuario:** Esta acción chequea si el dominio destinatario pertenece o no a la plataforma de correo, luego verifica si el usuario además existe en este dominio. Finalmente corrobora el estado comercial de la casilla (activo, inactivo, etc).

- **Control de e-mail por tiempo (tráfico):** Esta medida preventiva consiste en limitar la cantidad de correos que un usuario puede enviar en un período de tiempo determinado.

Por su parte un ISP en lo que a conectividad respecta no puede aplicar medidas de control sobre el sistema de correo, su rol queda supeditado sólo a responder solicitudes de identificación de aquellas IP con que ha sido emitido un correo, puesto que éstos salen con el IP de conexión del cliente. Bajo este contexto, el ISP se verá afectado si el envío de correo masivo se origina desde un IP del ISP, pues como consecuencia e inevitablemente será incorporado en una lista negra.

El resultado de que un número IP sea identificado en la Internet como emisor de correo masivo, es que estos son anotados en listas negras internacionales, las cuales son consultadas por muchos servicios de correo en el mundo, en otras palabras, a ese número IP le será bloqueado el

acceso a todos los servicios de correo que consulten esa lista negra. Medidas como éstas afectan en gran medida al ISP, en particular cuando realiza asignación de IP dinámica, puesto que se pueden presentar inconvenientes como que al próximo usuario que le sea asignado ese número IP tendrá problemas para enviar correo a Internet pues ese número IP se encuentra en una lista negra. Por otra parte, respecto del emisor de correo masivo, cuando se dé cuenta de que no puede enviar correo, lo más probable es que se desconecte y vuelva a conectar hasta que le sea asignado un número IP distinto (asignación dinámica de IP), por lo tanto seguirá emitiendo correo masivo.

Los ISPs nacionales pueden ayudar a construir listas negras nacionales, para ello deben compartir sus números IPs, de tal forma de dar a conocer al resto, aquellos emisores que no están autorizados para efectuar envío de correo. De esa forma un MSP controla chequeando que el IP que está realizando la conexión a su servicio de correo, no se encuentre en esa lista negra local.

II.- EL SPAM

1° Concepto

Como punto de partida, debemos decir que conceptualizar el SPAM, no es una labor simple, pues normalmente se dan conceptos amplísimos y sin mayor sustento tecnológico, que permiten introducir en tal concepto, variadas figuras, las cuales incluso pueden ser consideradas ética y legalmente aceptables, generando una confusión en quienes bandera en mano contra el SPAM y spammers, buscan a través de sus organizaciones mover los aparatos estatales, en busca de la dictación de sendas leyes que sancionen a los autores de estas prácticas, incluso en algunos casos proponiendo sanciones superiores a las que se pueden ver expuestos autores de crímenes o delitos de sangre.

Por ello a través de este acápite, trataremos de acercarnos a un concepto de SPAM, en cuanto tal, a fin de lograr un poco mas adelante, determinar que otras figuras podríamos encontrar relacionadas, afines o validas al respecto de las comunicaciones electrónicas no deseadas o no solicitadas, y que en estricto rigor no son los llamados SPAM.

En cuanto al SPAM en si, hay muchos que no han logrado establecer a ciencia cierta un concepto, pero han argumentado al tenor de una frase contenida en un fallo sobre pornografía de la Corte Suprema de Justicia de los Estados Unidos de Norteamérica, que señalo sobre la pornografía ***"No puedo definirla, pero la reconozco cuando la veo"***[3], en virtud de ello, con esta indeterminación conceptual, basada solamente en la casuística, los miembros de la comunidad antispam generalmente han preferido esta

3 Icauce.ar. [en línea] Argentina: Definición de Spam. [Fecha de consulta: 11 diciembre 2008] Ultima actualización 30 enero 2008. Disponible en: http://www.cauce.org.ar/Definici%C3%B3nDeSpam

definición de SPAM, que si bien la reconocen como débil y ambigua, les ha permitido sostenerla en el tiempo, y que sea aplicada de igual manera, debido a que los spammers han demostrado gran inventiva e iniciativa, en el tiempo, encontrados variadas maneras nuevas, diferentes y únicas para seguir adelante con sus acciones, pese a los esfuerzos de la comunidad.

El doctor en Derecho Constitucional **Ricard Martínez Martínez**,[4] con ocasión de un comentario doctrinal, respecto de la primera sentencia judicial en la República Argentina, que declaro ilegal en dicho país, entrega una definición de SPAM, basado en los elementos que este debe contener para ser considerado como tal.

Señala Martínez que, el SPAM propiamente dicho o correo basura consiste ***"en mensajes no solicitados de correo habitualmente remitido con intenciones comerciales",*** y agrega que para ser calificado como tal un mensaje de esta naturaleza debería reunir las siguientes condiciones:

1. no permite al destinatario dar de baja a futuro la suscripción;
2. el remitente es una persona difícilmente identificable;
3. en caso de envíos periódicos, éstos se realizan sin previa suscripción;
4. idéntico mensaje es enviado en forma masiva a personas que no lo han solicitado

Si bien Martínez se arriesga con un concepto y sus características, vemos que para determinar si el email que ha llegado a nuestra casilla de Correo Electrónico, debemos previamente analizarlo, es decir, sigue indirectamente la doctrina del fallo americano sobre pornografía.

---

4 Martínez Martínez, Ricard. SPAM. Comentarios a la luz de una reciente sentencia argentina. ***Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid,*** [en línea] Nº. 21, 2006. [Fecha de consulta 11 diciembre 2008] Pág.1 Disponible en http://www.datospersonales.org ISSN 1988-1797

Si seguimos avanzando en torno al concepto de SPAM, nos encontramos con más disquisiciones en torno a la materia, pues aparecen una serie de nociones agregando o eliminado componentes, exigiendo la concurrencia de determinados elementos, para poder hablar de SPAM propiamente tal.

En tal sentido si recurrimos nuevamente a la jurisprudencia internacional, nos encontramos con una sentencia de un Tribunal Colombiano, específicamente el Segundo Juzgado Promiscuo Municipal Rovira Tolima, de 21 de julio de 2003, en los autos caratulados **"Samper Posada c/ Tapias, Cediel y Otros"**[5]. En dicha sentencia se hace una distinción respecto del SPAM, exigiendo ciertos elementos casi de manera obligatoria, los cuales son la masividad y la existencia de un fin comercial, dejando de lado en uno u otro caso la característica de que sean correos **"no deseados o no solicitados".**

Al efecto expone el sentenciador ***"No existe una sola definición generalmente aceptada de spam. Definirlo como correo electrónico no deseado no elimina este problema. Al reflexionar sobre la regulación del spam no interesa, en verdad, saber si el correo es deseado o no. De lo que se trata es de decidir cuando resulta legítimo el envío de este correo no solicitado y cuando no. Tomada esa decisión, recién es posible preguntarse qué modalidades regulatorias y en qué medida pueden ser utilizadas para enfrentarlo. Aún cuando para algunos cualquier correo no solicitado es spam, las dos definiciones más aceptadas de spam son: correos electrónicos comerciales no solicitados CECNS[6] y correos***

5 CCIT.Org. Cámara Colombiana de informática y telecomunicaciones [en línea] Colombia. [Fecha de consulta: 15 enero 2008] Actualización permanente. Descargado de http://www.ccit.org.co/www/htm/descargas/documentos/fallo_tutela_spam.doc
6 Traducción del acrónimo de unsolicited comercial e-mail [UCE]

electrónicos masivos no solicitados CEMNS[7].”[8] Podemos observar, que para el sentenciador colombiano sólo habrá SPAM en estas condiciones, desechando cualquier otra carácter que no sea la masividad o referirse a una actividad comercial.

Continúa el sentenciador, en torno a la idea de “no deseado” al decir ***“Lo que resulta común en ambos casos es que se trata de correo electrónico no solicitado. Generalmente se ha entendido por no solicitado un correo en aquellos casos en que: no existe relación previa entre las partes y el receptor no ha consentido explícitamente en recibir la comunicación. Puede significar también que el receptor previamente ha buscado terminar una relación existente, usualmente instruyendo a la otra parte de no enviarle más comunicaciones en el futuro. Por supuesto no basta que se trate de correo no solicitado en los términos recién expuestos. Lo que, en principio, cualifica al correo no solicitado como spam es su carácter comercial, la cantidad enviada o, desde luego, una mezcla de ambos.”[9].*** Como podemos observar, el fallador es sumamente cauto, al definir “no solicitado”, incluyendo expresamente el caso de aquel usuario que se ha inscrito en una lista y ha pedido luego ser removido de las bases de datos, reconociendo expresamente el derecho que tenemos cada uno hacia los poseedores de datos y que han hecho la recogida de los mismos, de exigirles de acuerdo a la ley la eliminación de nuestros datos personales de dichos registros.

Agrega, ***“Aún cuando la definición de comercial varía en las distintas***

---

7 Traducción del acrónimo de unsolicited bulk email [UBE]

8 CCIT.Org. Cámara Colombiana de informática y telecomunicaciones [en línea] Colombia. [Fecha de consulta: 15 enero 2008] Actualización permanente. Descargado de http://www.ccit.org.co/www/htm/descargas/documentos/fallo_tutela_spam.doc

9 CCIT.Org. Cámara Colombiana de informática y telecomunicaciones [en línea] Colombia. [Fecha de consulta: 15 enero 2008] Actualización permanente. Descargado de http://www.ccit.org.co/www/htm/descargas/documentos/fallo_tutela_spam.doc

legislaciones del mundo, lo que suele considerarse en el caso de las comunicaciones comerciales es la promoción de algún tipo de bienes o servicios."[10] En dicho sentido cita expresamente, la Directiva 2000/31 de las Comunidades Europeas[11] define en su artículo 2 letra f) comunicaciones comerciales como: ***"todas las formas de comunicación destinadas a proporcionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización con una actividad comercial, industrial o de profesiones reguladas...".***

Despejado el tema "comercial" del mismo, el sentenciador respecto del carácter masivo se plantea dos interrogantes; la primera si debe tratarse del mismo mensaje enviado en forma multitudinaria para que califique como spam o puede tratarse de mensajes substancialmente similares; y la segunda, cuántos mensajes deben enviarse para que dicho envío sea considerado masivo.

En tal escenario, señala ***"Aún suponiendo que las definiciones de comercial y masivo no sean problemáticas, un inconveniente que subsiste es si el spam debe ser definido como CECNS o como CEMNS. Existen argumentos a favor de ambas posturas. En el caso de definirlo como CECNS: ¿Por qué el traslado de costos desde el emisor hacia el receptor de los mensajes es particularmente susceptible de objeciones en el caso comercial? ¿Si se define como CEMNS entonces resultará necesario fijar un umbral a partir del cual se trate de correo masivo?"*** [12]

---

10 CCIT.Org. Cámara Colombiana de informática y telecomunicaciones [en línea] Colombia. [Fecha de consulta: 15 enero 2008] Actualización permanente. Descargado de http://www.ccit.org.co/www/htm/descargas/documentos/fallo_tutela_spam.doc

11 Red Iris. [en línea] España. [Fecha de consulta: 10 septiembre 2007] Actualización permanente. Disponible en http://www.rediris.es/mail/abuso/ace.es.html

12 Red Iris. [en línea] España. [Fecha de consulta: 10 septiembre 2007] Actualización permanente. Disponible en http://www.rediris.es/mail/abuso/ace.es.html

Al respecto y basándose en el daño que produce el spam en si, el sentenciador razona si ***"En el caso de definirlo como CEMNS: El principal argumento es que el daño que se inflige con los correos masivos es absolutamente independiente de la naturaleza del mensaje. Los costos soportados por los receptores de los mensajes y las redes intermedias no poseen así relaciones con el contenido de la comunicación. Si de lo que se trata es de cautelar ese daño, distinguir según el contenido no tiene sentido. Por supuesto una tercera alternativa es definir spam como correo comercial masivo no solicitado."***[13]

Efectivamente, tal como se señala en esta misma sentencia a continuación, sin duda el spam es un gran negocio que invade casillas de correos electrónicos, equipos computacionales y servidores; ello gracias a los avances tecnológicos, que han permitido otorgar un acceso a internet mejorado y a sistemas de anchos de banda con tarifa plana. Esto sin duda ha beneficiado tanto, a los emisores como a los receptores. A los primeros obviamente porque le ha abierto la puerta a mas destinatarios, y a los segundos porque debido a las tarifa planas y la consecuente reducción del costo de recoger correo ya no es tan gravoso económicamente que la recepción de spam se asumen con resignación.

El mismo fallador, avanzado en su texto, y con ocasión de justificar el por que se estaría vulnerando una garantía constitucional y que haría aplicable la acción de Habeas Data en este caso señala ***"Sabemos que el spam es el envío indiscriminado de mails no solicitados. Si yo recibo un email que no solicite de una persona que no conozco, y que al***

13 Red Iris. [en línea] España. [Fecha de consulta: 10 septiembre 2007] Actualización permanente. Disponible en http://www.rediris.es/mail/abuso/ace.es.html

mismo tiempo es enviada a una cantidad de personas que tampoco lo solicitaron, eso es spam. No debería tener necesidad de enviar un email para que me borren de una lista ya que no deberían agregar mi dirección a ninguna de ellas, puesto que no he autorizado a estar incluido, es ahí en donde se me vulnera mi derecho constitucional y continúa la vulneración cuando comienzan a comercializar mi dirección electrónica, que tampoco he autorizado. Esta advertencia sólo se torna viable si el titular de la cuenta de correo electrónico ha autorizado recibir dichos mensajes, como cuando aceptamos recibir noticias o catálogos al cargar un software en nuestros equipos que ha sido bajado de la Internet"[14]. Agrega, ***"recibir spam, es como cuando encuentro un mismo vendedor golpeando insistentemente en mi casa, para ofertarme sus productos que vende, de los cuales no necesito, yo le replico no quiero nada suyo y le suplico a la vez no insistir ya que no me interesa su genero de productos. Nuevamente el mismo señor u otro personaje, me vuelven a ofrecer los mismos productos, los que no me interesan"***[15]. Es decir, no se trata sólo un daño en nuestros equipos, casillas, servidores, en nuestras economías, sino que se trata abiertamente de una intromisión en nuestra vida, en nuestra esfera de intimidad, lo cual obviamente, demuestra que poco interesa si el correo o comunicación es comercial o no, lo que si va tomando importancia es que va siendo un elemento que atenta contra mi derecho a la vida y a su intimidad, simplemente mi derecho a vivir tranquilo.

Sin embargo, tal construcción jurisprudencial no tiene cabida en todas partes, y por el contrario nos encontramos que en España, muchas

14 Red Iris. [en línea] España. [Fecha de consulta: 10 septiembre 2007] Actualización permanente. Disponible en http://www.rediris.es/mail/abuso/ace.es.html
15 Red Iris. [en línea] España. [Fecha de consulta: 10 septiembre 2007] Actualización permanente. Disponible en http://www.rediris.es/mail/abuso/ace.es.html

denuncias ante la **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS**[16], por presuntas acciones de spammers han sido desechadas por no ser comunicaciones comerciales.

Por ejemplo podemos citar el caso el **Expediente Nº: E/00075/2005**[17], por un denuncia contra la Asociación Foro Abril, la cual remitía artículos de índole periodístico a usuarios de emails en España. La señalada agencia dentro de la exposición de fundamentos de derecho señala en el II que ***"Actualmente, se denomina "Spam" o "Correo basura" a todo tipo de comunicación comercial no solicitada, realizada por vía electrónica." "De este modo, se entiende por "Spam" cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es el correo electrónico."***[18] Continua ***"Esta conducta es particularmente grave cuando se realiza en forma masiva. El envío de mensajes comerciales sin el consentimiento previo esta prohibido por la legislación española, tanto por la ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, como por la ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal."***[19]

Mas adelante en su considerando III señala el sentenciador que ***"La LSSI prohíbe las comunicaciones comerciales no solicitadas, partiendo de***

16 Ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones. Esta fue creada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Título VI con rango de ley ordinaria)

17 Agencia Española de Protección de Datos. Expediente Nº E/00075/2005 [en línea] España.[Fecha de consulta y descarga documento: 11 septiembre 2006] Actualización permanente. Disponible en https://www.agpd.es/upload/Canal_Documentacion/

18 Agencia Española de Protección de Datos. Expediente Nº E/00075/2005 [en línea] España.[Fecha de consulta y descarga documento: 11 septiembre 2006] Actualización permanente. Disponible en https://www.agpd.es/upload/Canal_Documentacion/

19 Agencia Española de Protección de Datos. Expediente Nº E/00075/2005 [en línea] España.[Fecha de consulta y descarga documento: 11 septiembre 2006] Actualización permanente. Disponible en https://www.agpd.es/upload/Canal_Documentacion/

un concepto de comunicación comercial que se califica como servicio de la sociedad de la información y que se define en su Anexo, apartado f), como: "toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional."[20]

Agrega además en el mismo considerando de Derecho, que en virtud del artículo 21 de la citada LSSI, según una modificación introducida por la disposición final primera de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, bajo el epígrafe: ***"Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes", establece que "queda prohibido el envío de mensajes publicitarios o promocionales por correo electrónico remitidos por persona o entidad que realice una actividad comercial, industrial, artesanal o profesional sin que hayan sido solicitados o autorizados expresamente por los destinatarios de los mismos, salvo que se trate de comunicaciones comerciales referentes a productos o servicios de la propia empresa que sean similares a los que inicialmente hubiesen sido objeto de contratación." .***

Finalmente en el considerando IV expresa que ***"en el supuesto examinado, se ha acreditado que en el período comprendido entre el 10/02/2004 y 12/03/2004, el denunciante recibió, en su buzón de correo electrónico profesional, ocho correos electrónicos no deseados remitidos desde diferentes dominios. En tres de ellos se hace***

20 Agencia Española de Protección de Datos. Expediente Nº E/00075/2005 [en línea] España.[Fecha de consulta y descarga documento: 11 septiembre 2006] Actualización permanente. Disponible en https://www.agpd.es/upload/Canal_Documentacion/

referencia al "Foro Arbil" o bien a la revista digital denominada "Arbil". En los correos de fechas 11 y 12/03/2004, el dominio remitente corresponde a "AB.AB" . Asimismo, consta que en los correos de fechas 10/02/2004 y 3/03/2004, se incita a acceder al dominio ".....A@....A..." . Continúa concluyendo que "del contenido de los correos se desprende que el denunciado no desempeña ninguna actividad comercial, industrial, artesanal o profesional, por lo que estos correos no pueden ser calificados como "comunicación comercial", a tenor de la definición contenida en el citado apartado f) del Anexo de la LSSI, pues no van dirigidos a promocionar una actividad comercial, industrial, artesanal o profesional. Por lo tanto, de acuerdo con el apartado a) del mismo Anexo, tampoco se trata de un servicio de la sociedad de la información, ya que para ello se requiere que la comunicación comercial se realice por una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional. Así las cosas, la remisión de estos correos electrónicos no ha podido acreditarse que supusiera infracción de la LSSI."[21]

De lo anterior, se nos abre una nueva puerta a esta disquisición en torno al concepto de SPAM, ya que aun cuando el correo enviado sea masivo, no deseado o solicitado, y su contenido no nos interese, al no tener un carácter comercial o publicitario para la legislación española no se trataría de SPAM.

Dicha tendencia, ha sido la que se ha ido popularizando internacionalmente, así por ejemplo podemos citar un proyecto de Ley de la República Argentina que buscaba establecer la **"PENALIZACION DEL**

21 Agencia Española de Protección de Datos. Expediente Nº E/00075/2005 [en línea] España.[Fecha de consulta y descarga documento: 11 septiembre 2006] Actualización permanente. Disponible en https://www.agpd.es/upload/Canal_Documentacion/

ECOMMERCE NO AUTORIZADO (SPAM) EN LA RED GLOBAL - INTERNET- EN EL AMBITO DE LA REPUBLICA ARGENTINA."[22] En dicho proyecto en su artículo 1º se señala lo siguiente ***"Denominase SPAM al e-commerce o comercio electrónico no autorizado de todo tipo de oferta de compra-venta de productos o servicios en general enviado mediante redes de correo electrónico sin consentimiento del usuario en la World Wide Web (www) o red electrónica global.".***

Por otra parte el mismo órgano legislativo también levantó otro proyecto de Ley que buscaba establecer el **"REGIMEN LEGAL PARA LAS COMUNICACIONES COMERCIALES POR VIA ELECTRONICA"[23].** En dicho proyecto se establece conceptos precisos de correo electrónico y de correo electrónico comercial. Dichos conceptos son definidos en el artículo 1º , como ***"Correo electrónico: toda correspondencia, mensaje, archivo, dato u otra información electrónica que se trasmite a una o mas personas por medio de una red de interconexión entre computadoras./ Correo electrónico comercial: todo mensaje emitido en forma electrónica por e-mail, cuyo principal propósito sea realizar publicidad y/o promoción de un producto o servicio con fines comerciales."*** **En tal orden de cosas establece en el artículo 2º que *"Queda prohibido en todo el territorio nacional el envío de comunicaciones publicitarias o promociónales por correo electrónico u otro medio de comunicación electrónica equivalente, que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas a través del consentimiento afirmativo.".*** De lo anterior podemos afirmar categóricamente que dicho proyecto también hace suyo el concepto de

22 PDP. Protección de Datos Personales. [en línea] Argentina [Fecha de consulta: 11 septiembre 2006] Actualización permanente. Disponible en http://www.protecciondedatos.com.ar/proyecto14.htm
23 PDP. Protección de Datos Personales. [en línea] Argentina [Fecha de consulta: 11 septiembre 2006] Actualización permanente. Disponible en http://www.protecciondedatos.com.ar/proyecto12.htm

SPAM reducido exclusivamente a las comunicaciones comerciales no solicitadas, y obviando el hecho de que sean masivos o no.

No obstante lo anterior, también en la Argentina, y en otro Proyecto de Ley sobre **"PROTECCION DE LAS DIRECCIONES ELECTRONICAS"[24],** el legislador por la vía de la excepción sanciona el envío de correos no publicitarios o comerciales no solicitados. En efecto en dicho proyecto los artículos 2º y 3º establecen ***"Queda prohibido en el territorio nacional la distribución, comunicación publicitaria o comercial mediante el uso del correo electrónico u otro medio de comunicación electrónica equivalente utilizando vínculos físicos como inalámbricos a destinatarios que previamente no hayan solicitado el envío de los mismos.(art.2º) Exceptuase de lo señalado en el artículo anterior a toda información no comercial previamente solicitada o expresamente autorizada por los destinatarios de las mismas y cuyos datos o direcciones electrónicas hayan sido obtenidas en forma lícita.(art.3º)"*** De lo anterior, queda claro, que al menos existe la intención de ampliar la protección, no sólo a los correos comerciales no deseados, sino también a los de cualquier otro tema no solicitados, lo cual permitiría sancionar muchos de los otros emails, que sencillamente se dedican a difundir una idea, propaganda política, doctrinas religiosas, etc, y el receptor no interesado se ve en la obligación de recibir, analizar y borrar, invadiéndose su privacidad, como ocurrió en el caso citado anteriormente en España.

En este escenario u orden de cosas, podemos citar la el proyecto de **"LEY DE PROTECCION RESPECTO DE LOS CORREOS ELECTRONICOS**

24 PDP. Protección de Datos Personales. [en línea] Argentina [Fecha de consulta: 11 septiembre 2006] Actualización permanente. Disponible en http://www.protecciondedatos.com.ar/proyecto15.htm

COMERCIALES NO SOLICITADOS"[25] del Perú. En dicho instrumento jurídico, nos encontramos con que el legislador incluyó originalmente de manera expresa en el concepto de correo comercial, aquellos que tengan por fines la promoción política o religiosa. En efecto, el artículo 2º al entregar las definiciones para la aplicación de dicha ley, señala en la letra b) inciso primero que ***"Correo electrónico comercial: Todo correo electrónico que contenga información, falsa o real, dedicada a la promoción o publicidad, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional, o cualquier otra con fines de lucrativos."*** Dicho concepto muy apegado al concepto español de correo electrónico comercial, se modifica sustancialmente con el inciso segundo que señala ***"También se considera como correo electrónico comercial aquel que contenga promoción o publicidad de organizaciones políticas o religiosas."***

En este sentido el legislador del Rimac, abría una puerta más ancha a la protección de la intimidad, al ampliar el ámbito de aplicación de ley y de protección, a otras actividades que normalmente quedan excluidas de persecución, y que son tan molestas o invasoras de nuestra privacidad como las comerciales.

No puedo negar, que si bien la técnica legislativa no era muy depurada, daba un paso bastante grande en lo que se refería a proteger de mayor y mejor manera la intimidad en general de las personas y no sólo de los abusos de correo electrónico comercial no solicitado; puesto que es sabido, que existen correos que al borrarse por el usuario o el mero hecho de

25 Indecopi. Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [en línea] Perú. [Fecha de consulta: 11 septiembre 2006] Actualización permanente. Disponible en http://www.indecopi.gob.pe/antispam/ley-antispam-peruana.html

solicitar la remoción de la base de datos, sólo están validando su propia dirección de casilla de correo ante los spammers; y de una u otra manera están entregando o confirmando información de datos personalísimos o datos personales sensibles, como podrían ser las tendencias políticas o religiosas de una persona. Y con la redacción dada originalmente al proyecto, permitía un avance a esa protección, pues ampliaba el ámbito de acción de la legislación.

Desgraciadamente la ley que vio la luz en el vecino país, no consideró dicha ampliación y optó por una definición tradicional de correo electrónico comercial, al definirlo como ***"Todo correo electrónico que contenga información comercial publicitaria o promocional de bienes y servicios de una empresa, organización, persona o cualquiera otra con fines lucrativos"***[26]

Si seguimos por este camino, en nuestro país, no se ha avanzado mucho, y no existe ley que entregue un concepto se SPAM. Uno de los primeros intentos, lo encontramos es una breve conceptualización de este, en un mensaje de un proyecto de ley[27] que perseguía modificar la Ley Nº 19.628, sobre "**PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**" para introducir el concepto de uso indebido o abusivo de datos. En dicho proyecto se señala en su mensaje al respecto que **"*El correo Spam es una modalidad de correspondencia electrónica que se utiliza para el envío de publicidad no solicitada*".** De lo anterior, podemos ver que el legislador nacional ha seguido simplemente, la doctrina que identifica al SPAM con los correos comerciales y que además no hayan sido solicitados.

---

26 Diario Oficial El Peruano. Ley Nº 28.493, que regula el uso del Correo electrónico comercial no solicitado (SPAM) [en línea] Perú. [Fecha de consulta: 14 septiembre 2006] Actualización permanente: Disponible en. http://www.elperuano.com.pe/

27 BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 3095-07. [en línea] Chile. [Fecha de consulta: 3 Marzo 2008] Actualización permanente. Disponible en: http://www.bcn.cl/

Por otra parte, también encontramos en otro proyecto de Ley, también destinado a modificar la ley Nº 19.628, conocido como el Proyecto Novoa[28]. En dicho proyecto se perseguía modificar la ley señalada, incorporando las direcciones de correo electrónico como dato de carácter personal sensible, de manera de atacar específicamente el problema del SPAM, iniciativa parlamentaria que de momento no analizaremos en mayor profundidad.

En tal sentido, acertadamente señala el legislador que no existe un concepto unánime del anglicismo "spam", pero a efectos de dicha Moción se le concibe como ***"todo correo electrónico enviado de forma masiva, sin autorización del titular de la dirección o casilla electrónica, obteniéndose las direcciones de correos de fuentes no públicas de información, y que ocasiona perjuicios económicos al receptor de la comunicación, independientemente de que su contenido se relacione -o no- con una promoción comercial u oferta de servicios".***

Este concepto nacional merece variados comentarios. En primer lugar considera la **"*masividad*",** que en el proyecto anteriormente fue obviado o dado como de la esencia de la figura. En segundo lugar, agrega la falta de **"autorización del titular de la dirección o casilla electrónica**"; es decir, el que sea no deseado o no solicitado. En tercer lugar, podríamos decir que entramos en problemas, ya que agrega un carácter propio, quizás algo antojadizo para que el concepto permita por si mismo su justificación en este proyecto de ley. En efecto, agrega **"obteniéndose las direcciones de correos de fuentes no públicas de información"**, con lo cual cualquier spammer que se persiguiera, podría hacer presente que obtuvo la información de una fuente pública de información. Por ejemplo muchas

28 BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 3796-07. [en línea] Chile. [Fecha de consulta: 3 Marzo 2008] Actualización permanente. Disponible en: http://www.bcn.cl/

personas, publican su dirección de email en los directorios de páginas amarillas, en busca de mejorar sus posibilidades de contacto cuando ofrecen algún servicio técnico-profesional. Estos directorios son reconocidos por todos como fuentes públicas de información. Acaso ello implica que estoy diciendo "envíeme todo lo que quieran, aun ofertas que no me interesan". La verdad que no es ese el objetivo de un aviso así, es recibir cotizaciones de sus servicios, resolver inquietudes de sus clientes, etc.

En cuarto lugar, se señala como característica del SPAM nacional, el hecho de "**que ocasiona perjuicios económicos al receptor de la comunicación"**. Aquí el problema estriba, en que los perjuicios en la legislación nacional no se suponen de pleno derecho, y por lo tanto, para que pudiéramos definitivamente condenar a un spammer como tal, deberíamos en primer lugar lograr acreditar perjuicios y que los tribunales así los declararan. Una cosa que no hay que perder de vista, es que efectivamente el SPAM puede causar perjuicios en muchos ámbitos, tanto a los ISP's, MSP's, servidores, usuarios del servicio de correo electrónico, etc; pero dentro del proyecto citado, el objetivo era la invasión de la privacidad, la cual en mi modesto parecer, si invade exactamente igual, con o sin perjuicio económico.

Por último, agrega como elemento y acercándose mas al modelo peruano el hecho de que **"*independientemente de que su contenido se relacione -o no- con una promoción comercial u oferta de servicios*",** con lo cual obviamente incorpora cualquier contenido u objeto del mensaje enviado.

Obviamente podríamos seguir profundizando en este concepto, pero sin lograr llegar a buen puerto, pues la infinidad de opiniones en la materia, tanto de profesores, legisladores o jueces es muy abundante, y hace especialmente interminable el asunto.

Por la problemática planteada, es que los expertos (no jurídicos) han construido un concepto dotado de mayor precisión, al menos según sus dichos, señalando que ***"Internet spam is one or more unsolicited messages, sent or posted as part of a larger collection of messages, all having substantially identical content."***[29] , que en nuestra lengua significaría que "El spam de Internet es uno o más mensajes no solicitados, enviados o despachados como parte de una gran colección de mensajes, los cuales todos tienen un contenido esencialmente idéntico". Como podemos observar, en dicho concepto, poco importa su contenido, sino que se atiende a su masividad.

Siguiendo la misma línea, dicho concepto y con una profundidad similar, fue tomado por la Corte Suprema de Washington el año 2001 y señalo que ***"The term 'spam' refers broadly to unsolicited bulk e-mail (or "junk e-mail'), which 'can be either commercial (such as an advertisement) or noncommercial (such as a joke or chain letter)."*** [30], es decir, "El término el "Spam" se refiere ampliamente al E-mail a granel no solicitado (o el correo basura), el que puede ser comercial (por ejemplo un anuncio) o no comercial (por ejemplo una broma o una cadena)." Como podemos observar, este concepto jurídico nacido del seno de los Tribunales Norteamericanos, tomo como elementos esenciales la masividad y, la no petición del receptor, señalando expresamente que poco importa si es comercial o no.

De lo anteriormente expuesto en este numeral, nos hemos encontrado, con que para la doctrina nacional e internacional, existen distintas

29 Twelve Horses. Anti_spam Policy. [en línea] . EEUU. [Fecha de consulta: 5 Marzo 2007] Actualización permanente. Disponible en: http://web.twelvehorses.com/terms/antispam/
30 Infinite Monkey & Company. Spam Defined. [en línea] EEUU. [Fecha de consulta: 5 Marzo 2007] Actualización permanente. Disponible en: http://www.monkeys.com/spam-defined/

comunicaciones, que para unos pueden ser SPAM o no, pero que en si constituyen los llamados abusos de correo electrónico, los cuales analizaremos en el numeral siguiente.

Finalmente a este respecto la **NACPEC**[31], señala que el Spam es ***"el correo comercial no solicitado generalmente enviado a las direcciones electrónicas de los consumidores sin la autorización y consentimiento del consumidor, comúnmente es enviado por empresas de mercadeo o telemercadeo, compañías legítimas o por individuos comisionados exclusivamente para dicho fin"***[32]

Asimismo, y es de suma importancia señalar que solemos ver el problema del SPAM, sólo desde la óptica de los correos electrónicos, pero eso es una postura poco feliz; ya que es un hecho que el actual mundo de las comunicaciones electrónicas y la interconectividad entre un servicio y otro, así como la existencia de redes globales, dicha óptica es estrecha, ya que es un problema que afecta muchos mas sectores, tal como el Internet, las telecomunicaciones locales e internacionales, fijas y móviles, los servicios de mensajería instantánea, etc, hecho que ya en variadas legislaciones se reconoce, y que en Chile hasta la fecha no nos habíamos preocupado, hasta una moción del Senador Jaime Naranjo[33], que presento un proyecto de Ley que busca regular la publicidad en las llamadas telefónicas, para lo cual se busca modificar la Ley 19.496 Sobre Protección de los Derechos de los Consumidores, específicamente en su artículo 28 B. En efecto se propone en un artículo único incorporando como incisos 3,4 y 5 del

31 El Proyecto Norteamericano sobre Protección al Consumidor en Comercio Electrónico (NACPEC) es una organización Mexicana, que fue inicialmente creado con el propósito de ofrecer fuentes de información sobre comercio electrónico para consumidores ubicados en Norteamérica. Sin embargo, tomando en cuenta que el alcance de la legislación sobre Internet y la elaboración de política es de naturaleza global, NACPEC se ha ampliado con el objeto de cubrir y proporcionar fuentes de información sobre protección al consumidor en comercio electrónico de la Unión Europea y de otros países líderes en el área.
32 NACPEC. Preguntas más frecuentes acerca del Spam y Phising, [en línea] EEUU: [Fecha de consulta: 5 Marzo 2007] Actualización permanente. Disponible en: http://www.nacpec.org/es/faq.html
33 BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 4844-06. [en línea] Chile. [Fecha de consulta: 5 Marzo 2007] Actualización permanente. Disponible en: http://www.bcn.cl/

artículo 28 B recién citado lo siguiente ***"Toda llamada efectuada por proveedores que dirijan comunicaciones promociónales y publicitarias a los consumidores por medio de fax, o servicios de mensajería telefónica, deberán ser efectuadas a través de una línea única que permita a los usuarios de teléfonos fijos y celulares solicitar a las empresas telefónicas el bloqueo de éstas de una sola vez y en forma definitiva. Será responsabilidad de la Subsecretaría de Telecomunicaciones implementar el reglamento respectivo."***

"Así mismo se deberá implementar un Registro Nacional donde las personas dueñas de teléfonos fijos y celulares dejaran establecido su voluntad de no recibir llamados telefónicos publicitarios de cualquier tipo. La inscripción en este registro será gratuita y durará 5 años. Las empresas que realicen publicidad mediante esta vía deberán obligatoriamente consultar este registro."

"Serán responsables del cumplimiento de estas normas tanto la empresa que realiza la llamada publicitaria como su mandante y, el incumplimiento devengará multas similares a las establecidas en el artículo 24, inciso primero, de esta misma ley."

En el mismo orden de cosas, otro proyecto actualmente en tramitación que modifica las leyes Nº 19.496, y Nº 19.628 con el objeto de regular el envío de correos electrónicos y de llamadas o "spams" telefónicos de carácter comercial y/o publicitario; el cual analizaremos más adelante de este trabajo, pero reproduciremos a continuación su considerando décimo por cuanto recoge parte de lo ya expresado en este trabajo: ***"Una derivación del "spam" viene dada por el "spam" telefónico o la realización de propuestas comerciales no solicitadas y reiteradas por teléfono u otros medios de comunicación. Es una de las prácticas más comunes***

que utilizan las empresas para ofrecer, promocionar, publicitar algún producto o servicio. Este tipo de publicidad no deseada es un fenómeno mundial, se traduce en millones de llamadas telefónicas importunando a miles de personas y constituyendo una manera desleal de hacer publicidad y de ofrecer un producto o servicio. En efecto, la comunidad europea en su directiva 2005/29/CE, ha calificado a los "spam" telefónicos como agresivos e ilegales, ya que se considera que toda publicidad tendiente a que el consumidor tome una decisión sobre una transacción que de otra forma no hubiere tomado, constituyen prácticas engañosas y desleales."[34]

2°.- Figuras anexas al Spam

En este numeral, revisaremos todas aquellas comunicaciones que posiblemente el común de los mortales calificaríamos como SPAM, y que según la interpretación del autor debieran estar incluidas bajo el concepto de SPAM, mas allá de su masividad, no solicitud, su carácter comercial, etc.

En doctrina se dice por algunos que existe el SPAM y que este sería parte de los llamados **ABUSOS DE CORREO ELECTRONICO** o según sigla **ACE**. Este es definido por el profesor **Jesús Sanz de Las Heras**[35] como "las diversas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios". Agrega el mismo Sanz que ***"algunos de los términos habitualmente asociados en Internet a estos tipos de abuso son spamming, mail bombing,***

---

[34] BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 6136-03. [en línea] Chile. [Fecha de consulta: 2 Noviembre 2008] Actualización permanente. Disponible en: http://www.bcn.cl/

35 Sanz de Las Heras. Jesús. Abusos en el correo electrónico. Ponencia en II Seminario Complutense de Telecomunicaciones e Información Madrid, Diciembre 1998 /[en línea] España. [Fecha de consulta: 5 Marzo 2007] Pág.1 Disponible en: http://www.ucm.es/info/dinforma/activi/libro/9.html

unsolicited bulk email (UBE), unsolicited commercial email (UCE), junk mail, etc., abarcando un amplio abanico de formas de difusión".

Tal como señala Sanz de Las Heras, nos encontramos con esta serie de instituciones, que pese a inundar nuestro correo, no obedecen necesariamente al llamado SPAM, sino que tal como su nombre lo indica un abuso.

Al respecto nos encontramos con las siguientes figuras, posiblemente ampliamente conocidos por todos, pero tal como indique para la mayoría de las personas serían SPAM's, o tienen al menos un pequeño aroma a ello.

Es tan claro el hecho que para el común de las personas no distingue entre un SPAM, un abuso de correo electrónico, un mail-bomb, una prospección comercial, etc, para ellos siempre es SPAM. Esto lo podemos comprobar viendo estadísticas internacionales. Así por ejemplo la profesora **Ana Brian Nougrères** en el X Congreso Iberoamericano de Derecho e Informática, celebrado en Chile en septiembre de 2004, presentó un ponencia denominada ***"¿Dis-función o de-función en la red de redes?"***[36]. En dicha ponencia, señalaba textualmente ***"partiendo del supuesto de que si no existe una conducta socialmente reprobable es muy difícil punir, es muy difícil sancionar"*** invitaba a continuación a observar una cuadro, que mostraba la definición de Spam a nivel de ciudadano común, la cual nacía expresamente del desconocimiento de la gente, y lo definían como Spam dependiendo del emisor y el asunto de que

36 Brian Nougrères, Ana . ¿Dis-función o de-función en la red de redes?. Memorias del X Congreso Iberoamericano de Derecho e Informática, celebrado en Chile en septiembre de 2004.Pág.273 y ss. Santiago. Chile. ISBN: 956-299-327-2

tratara.

En dicho cuadro se incluían expresamente los correos comerciales no solicitados, los que ofrecían asesorías financieras, los correos que pertenecían grupos políticos o defensas ciudadanas, los mensajes con contenido religioso y partidista, y aquellos mensajes con contenido adulto, entre otros.

Agrega a continuación, quizás la esencia de el por qué de esta confusión, al referirse a la finalidad del email enviado. En efecto señala ***"si la finalidad es el engaño, el fraude, no cabe duda que existe una conducta ilícita, que debe ser perseguida, y nuestros esfuerzos han de ser en el sentido de otorgar coercibilidad a las normas y darles mayor fuerza ejecutiva"*** Continua, ***"ahora bien, si se trata de Spam realizado con finalidades comerciales, con la única motivación de acceder a un número importante de potenciales consumidores de determinados productos, si bien esta conducta muchas veces es atentatoria de la privacidad, no se trata de una conducta que haya sido condenada unánimemente en los distintos foros internacionales donde se han debatido estos temas".*** De lo anterior queda de manifiesto, que estos mensajes no deseados, por el mero hecho de que lo sean, para ellos constituyen Spam, más allá que se trate de una ilicitud como ocurriría en un engaño o una simple oferta comercial.

Todos estos tipos de emails, llamados comúnmente por las personas como Spam, son tal como se señalo antes los llamados ACE o Abuso de Correo Electrónico.

Dentro del SPAM propiamente tal, la doctrina reconoce las siguientes acciones:

El **SCAM O JUNK MAIL**[37], el cual es similar al spam, que se utiliza para referirse a correos relacionados con publicidad engañosa, tales como los de enriquecimiento al instante, pornografía, premios, etc; y las infaltables cadenas, tales como aquellos correos que incluyen textos en donde solicitan ser reenviados a otras personas con la promesa de cumplir deseos, traer buena suerte, salvar el amazonas o ganar dinero.
Además del Spam, actualmente y por la proliferación de los servicios de mensajería instantánea, llamados comúnmente Chats, han aparecido los **SPIM**[38], que es un tipo de Spam destinado a estos servicios.

La doctrina internacional reconoce como formas de ACE, aparte del Spam los siguientes:

- **Difusión de contenido inadecuado.** Estos son aquellos cuyo contenido es ilegal por naturaleza, es decir, todo el que de una u otra manera constituye autoría o complicidad con hechos delictivos. Tales son:
    - ***Aquellos que hace apología al terrorismo;***
    - ***Aquellos que contienen programas piratas o que contienen cracks para vulnerar derechos de propiedad intelectual de softwares licenciados***
    - ***Aquellos que contienen pornografía infantil o direcciones a sitios relacionados con ella;***
    - ***Aquellos que contienen estafas o fraudes, como los llamados hoaxed, los de ingeniería social, fraude nigeriano, etc***
    - ***Aquellos que contienen virus o código maliciosos en***

37 Téllez Valdés, Julio. Regulación del spam en México. [en línea] México. [Fecha de consulta y descarga documento: 22 Marzo 2006] Disponible en: http://www.razonypalabra.org.mx/anteriores/n49/bienal/Mesa%205/JulioTellez.pdf.
38 Téllez Valdés, Julio. Regulación del spam en México. [en línea] México. [Fecha de consulta y descarga documento: 22 Marzo 2006] Disponible en: http://www.razonypalabra.org.mx/anteriores/n49/bienal/Mesa%205/JulioTellez.pdf.

general, etc

- **Difusión a través de canales no autorizados:** A estos se refiere aquellos que se envían desde un servidor ajeno, para reenviar correos propios, aun cuando el mensaje en sí sea legítimo, se están utilizando recursos ajenos sin su consentimiento.

- **Difusión masiva no autorizada.** El envió a través de servidores propios o ajenos de material masivo publicitario o no, no solicitado, traspasando el costo de sus operaciones a los destinatarios, ESP e ISP.

- **Ataques con objeto de imposibilitar o dificultar el servicio de correo electrónico.** Estos son aquellos que se caracterizan por estar dirigidos a un usuario o al propio sistema de correo. En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga el objetivo neto de paralizar el servicio por saturación de las líneas, de la capacidad de CPU del servidor, o del espacio en disco de servidor o usuario. Un claro ejemplo de estos también son aquellos de **"Suscripción indiscriminada a listas de correo",** en el cual de forma automatizada se suscribe a la víctima a miles de listas de correo. Dado que en este caso los ataques no vienen de una sola dirección, sino varias, son mucho más difíciles de atajar.

Además dentro de estos encontraremos mezclas, tomando elementos de uno u otro, actividades propias de los spammers y de los autores de abuso de correo electrónico, las cuales son acciones a través de las cuales van innovando de manera de evitar ser detectados por los usuarios o por los filtros o listas negras, respecto de estos últimos hablaremos mas adelante.

Dentro de estas combinaciones encontramos los llamados emails que dan lugar a la figura delictual muy vigente hoy en día del **PHISHING**. Este deriva su nombre de la contracción inglesa "**PASSWORD HAVERSTING FISHING**" que quiere decir "***pesca y cosecha de contraseñas, a través de la creación de réplicas de páginas web para literalmente "pescar" a los usuarios y hacerles enviar información personal, financiera o contraseñas***"[39]. Es una variante de lo que antes se conocía como Ingeniería social[40], la cual consiste en engañar a los destinatarios de email a abrir mensajes, dar contraseñas o proporcionar información confidencial, aprovechándose de su curiosidad, credulidad o inexperiencia informática. Estos obviamente nos encontramos ante comunicaciones que buscan la comisión de delitos, pero hay otros que se basan de métodos ilícitos, basados en intereses comerciales, como los que recurren a trampas del tipo **CAMUFLAGE O MUNGING**[41], las cuales son técnicas de ocultación de datos por parte de los spammers para evitar ser detectados. También tiene lugar cuando los destinatarios del email usan HTML o Javascript para camuflar enlaces de email y direcciones de correo para que las direcciones se puedan leer y se pueda hacer clic sobre ellas, pero no pueden ser recolectadas.

Otra figura que puede ser delito o no, y que puede tener por objeto cualquiera imaginable, y que es muy utilizado por los adolescentes casi como vendetta siciliana es el **JOE JOB** o mensaje incriminatorio[42], el cual es una campaña de spam falsificada para que aparente proceder de una parte inocente, con la intención de incriminarlo, a fin de que se vea

39 Glosario de términos sobre Internet y Spam. en línea] España. [Fecha de consulta: 22 Marzo 2006] Disponible en www.agpd.es/index.php?idSeccion=541
40 AEDI. Asociación Española para la Dirección Informática. Glosario de Spam.[en línea] España. [Fecha de consulta: 22 Marzo 2006] Disponible en http://www.aedi.es/asp/ANOT-0101.asp?NumeroN=168
41 AEDI. Asociación Española para la Dirección Informática. Glosario de Spam.[en línea] España. [Fecha de consulta: 22 Marzo 2006] Disponible en http://www.aedi.es/asp/ANOT-0101.asp?NumeroN=168
42 AEDI. Asociación Española para la Dirección Informática. Glosario de Spam.[en línea] España. [Fecha de consulta: 22 Marzo 2006] Disponible en http://www.aedi.es/asp/ANOT-0101.asp?NumeroN=168

inundada con un aluvión de mensajes devueltos por la campaña de spam.

Como podemos observar, existen variadas formas de ACE específicamente, llamados Spam por el común de las personas, y que de una u otra manera se relacionan por no ser solicitados, por ser masivos y por ser ilícitos o encontrarse en una posición muy cercana a dicha ilicitud. Pero existen aun una serie de comunicaciones electrónicas masivas, que no necesariamente quedan englobadas en el concepto o idea de ACE, son aquellas llamadas comunicaciones de prospección comercial.

Estas prospecciones comerciales, son una de las técnicas del marketing, y en especifico del telemarketing, las cuales tienen por objeto la comercialización y distribución de un producto entre los diferentes consumidores, de manera de que el productor diseñe y distribuya bienes de consumo que satisfagan las necesidades del consumidor, o que estos crean que satisfaceran sus necesidades.

Ya hemos visto que en general a nadie le gusta que su E-MAIL se inunde con ofertas publicitarias no solicitadas, pero una nueva forma de anuncios por correo electrónico está dando resultados y aquéllos a quienes se dirige incluso la reciben con agrado.

El telemarketing por correo electrónico llamó la atención por primera vez hace unos años, cuando los consumidores se quejaban de los anuncios no solicitados que inundaban sus buzones. Muchas empresas decidieron como estrategia el dejar dicha acción y reemplazarla por una donde el cliente voluntariamente aceptara recibirlos.

Según el experto en marketing, **Juan Manuel de la Colina** en un artículo

publicado en la web[43], señala que ***"al respecto un estudio de marzo de 2004 de la firma de investigación Forrester Research, la mayoría de las compañías que usan el correo electrónico opcional en su estrategia de marketing lo hace a través de herramientas propias con muy poca personalización."***

El mismo Colina cita a un prestigioso analista de **Forrester, Paul Sonderegger,** quien dijo que ***"los mensajes de correo electrónico orientados a mantener a los clientes ya existentes son más efectivos. En la retención, uno sabe algo" sobre su cliente. Ahí es donde el correo electrónico es más poderoso: en comunicarse con la gente de acuerdo con sus intereses y ponerse cada vez más a tono con esos intereses"***[44]

A raíz de esta consideración han aparecido en España con mucha fuerza, empresas dedicadas a la prospección económica comercial, bajo la forma de empresas de email marketing.

El Email Marketing también se le denomina **Marketing Autorizado o Permission Email Marketing**, y para sus sostenedores es una técnica muy efectiva de publicidad on line y nada tiene que ver con el envío de mensajes no solicitados o spam, ya que básicamente consiste en el envío de comunicaciones promocionales vía correo electrónico al buzón privado de las personas que han manifestado expresamente su interés por recibir estas comunicaciones, y según sus propios dichos ***"el destinatario***

43 De la Colina, Juan Manuel. Importancia, desarrollo y evolución del Marketing. Wikilearning. Comunidades de wikis libres para aprender. [en línea] Sin información país de origen. [Fecha de consulta: 5 Marzo 2007] Disponible en: http://www.wikilearning.com/introduccion-wkccp-4372-1.htm

44 De la Colina, Juan Manuel. Importancia, desarrollo y evolución del Marketing. Wikilearning. Comunidades de wikis libres para aprender. [en línea] Sin información país de origen. [Fecha de consulta: 5 Marzo 2007] Disponible en: http://www.wikilearning.com/introduccion-wkccp-4372-1.htm

acepta un envío continuado de mensajes que paulatinamente genera una relación de confianza con la empresa emisora."[45]

La importancia de este sistema, se explica en un estudio patrocinado por la Comisión Europea, el cual señala que el valor de una de estas campañas es sólo de un 10% del valor de una campaña por correo físico tradicional; siendo sus tasas de respuesta efectiva entre el 5% y el 15%, mientras que las de los mailings tradicionales se sitúan entre el 0,5% y el 2%. Agrega este mismo estudio que "el marketing por correo electrónico alcanza tasas de click-through o pulsación efectiva de alrededor el 18%, mientras que los banners publicitarios, según diversos estudios, no llega al 1%"[46]

Esto se produciría por varias razones. La primera correspondería a que los mensajes son personalizados lo cual permite segmentar el mercado, y en segundo lugar, porque el usuario se siente especialmente atendido y respetado, y no invadido en su intimidad.

3.- Problemática técnico jurídica del Spam

Habiendo intentado separar la crema de la leche, es decir, definir el Spam e intentar distinguirlo de las demás figuras afines.

Nos referimos a un análisis técnico jurídico, lo cual es necesario para completar esta Actividad formativa equivalente a Tesis, de acuerdo a los objetivos planteados, permitiendo además proponer una legislación

45 Senyal. Internet multimedia. Email Marketing. La publicidad on line efectiva. [en línea] España. [Fecha de consulta: 5 Marzo 2007] Disponible en: http:// www.senyal.com/esp/email_marketing/
46 Senyal. Internet multimedia. Email Marketing. La publicidad on line efectiva. [en línea] España. [Fecha de consulta: 5 Marzo 2007] Disponible en: http:// www.senyal.com/esp/email_marketing/

adecuada.

A modo de introducción de este tema, debemos señalar que nos encontraremos con una serie de problemas a resolver en forma previa, a fin de lograr dilucidar si es realmente factible regular el Spam de una manera efectiva, los cuales dicen relación con la problemática técnico jurídico.

El primer problema que avizoramos es definir el objeto que se hace necesario regular. Si nuestra respuesta es simplemente el Spam, ello no deja de ser complicado, ya que como hemos podido advertir de la exposición anterior, el legislador, tanto nacional como internacional, no están contestes en el concepto ni la extensión dada al mismo, y una regulación indiscriminada obviamente puede resultar atentatorio a muchas personas que ejerzan una actividad licita de email marketing.

Por otra parte, y suponiendo que el legislador efectivamente, logre determinar que es el Spam, y que ello no atente contra estas empresas legitimas de email marketing, que ocurrirá con aquellos abusos de correo electrónico, que si bien no son considerados Spam, como ocurre en la legislación española, en que si no se trata de un correo con contenido publicitario comercial no es sancionado. Surge entonces la pregunta ¿por que tendríamos que aceptar que se invada nuestra vida y su consiguiente intimidad y tranquilidad?, con mensajes políticos, religiosos, o de alguna seudo campaña humanitaria, etc. ¿Acaso la molestia no es la misma?. Obviamente esta amenaza aparece según mi criterio como mas grave, pues a través de esos mensajes y algunas operaciones de cruza de datos se puede obtener indirectamente por técnicas tanto manuales como automatizadas, datos personales de carácter sensible, que sólo a nosotros mismos nos interese conocer, y por consiguiente revelar a quienes

consideremos nosotros mismos como dignos de conocer nuestras verdades, y mantener el derecho a la **AUTOIMAGEN**[47] ante terceros extraños. En consecuencia, el segundo problema es determinar si nos interesa limitar sólo las comunicaciones comerciales no deseadas o nos interesa proteger la intimidad de una persona en su real extensión?

Sin duda un tercer gran problema, y que viene de la mano de los anteriores, unido al hecho de que el Spam se trata de un problema **EXTRATERRITORIAL**, es lograr hacer coincidir al máximo las distintas legislaciones internacionales sobre la materia, tomando en cuenta que para ello, existen países que lo sancionan, otros que intentan hacerlo, y otros para los cuales prácticamente no es un tema, que valga la pena el desgaste legislativo.

Uno de las primeras cuestiones a tener en vista, es que pese a que el Internet y el spam son propios de un mundo privado, y para muchos en un comienzo estaba fuera de las leyes y regulaciones internacionales, siendo realmente un mundo virtual (como contraposición al mundo real, reglado y sancionado en sus conductas) no se puede olvidar que afecta a millones de usuarios de todos o casi todos los países del orbe, tanto en lo que respecta a los derechos y garantías constitucionales de esas personas, como los derechos y patrimonios de los distintos operadores de redes y en general de todos los actores de este mercado.

Esta actividad en comienzos netamente académica y universitaria, a medida que fue creciendo fue estableciendo las llamadas ***"Netiquettes"* o *"prácticas de buenas costumbres y usos",*** las cuales posiblemente en los albores de esta red, eran suficientes y bastaban para evitar problemas o abusos en la red en si y en sus servicios anexos. Luego con la explosión

47 Chile, solicito en 1992, ante la OEA la inclusión del Derecho a la Autoimagen en todos los textos Constitucionales de los países Miembros: Informe Anual de la Comisión Interamericana de Derechos Humanos.

de empresas que vieron en el acceso a Internet una fuente de negocios, estas mismas llamadas **ISP's** (Internet Services providers) comenzaron a establecer sus propias normas, de manera de que quienes contrataran con ellos, mantuvieran ciertos cánones de conducta en la red, y evitaran o se abstuvieran de realizar determinadas acciones. Surgieron en la red comunidades de todo tipo, compuestas por personas de todas las edades, sexos, ideas e intereses, desapareciendo el espíritu o ideario académico, y estas reglas fueron cada vez menos respetadas, sin entrar a considerar la existencia de personas organizadas o no, que al igual que como en todo ámbito de la vida, veían una forma de hacer negocios, y otros de sacar provechos ilícitos, de obtener ventajas fraudulentas o simplemente dañar. Acciones, como estas se comenzaron a dar hace ya varios años, amparados en la ignorancia de los mismos usuarios, en la creencia de la llamada **"OPACIDAD DE LA RED",** que hacía que muchos se sintieran seguros en sus casas, manteniendo conversaciones con absolutos desconocidos o entregando información a supuestas empresas u organizaciones, con los más variados fines.

De lo anterior, surge la interrogante, ¿Por qué el Estado debería preocuparse por legislar estas actividades virtuales?, ¿En qué momento esta actividad privada, pasa a necesitar la tutela de la ley y a no ser capaz de autoregularse?

Además, hay que unir que a lo anterior, en ciertos países, quizás aquellos tercermundistas o en vías de desarrollo, o aquellos países que se vieron enfrentados a regímenes autoritarios o totalitarios, donde los conceptos de garantías constitucionales eran muy básicos, en que sólo aspirábamos a vivir, y con ello me refiero, a saber que si salíamos de nuestra casa en la mañana, al terminar el día, la familia se reuniría nuevamente, y no habría que lamentar muertes, detenciones o las usuales desapariciones de

personas. A que apunto con ello, es que en estos países, sus habitantes, desconocían o desconocen hasta el día de hoy, su derecho a la intimidad y a su privacidad, y que sea cual sea la forma en que se ataque, exactamente igual esta protegido por la Constitución y las leyes. Quizás la mejor manera de darnos cuenta de este problema, viene dado por el hecho de observar a la gente o a nosotros mismos. Por ejemplo, cuántos de nosotros no hemos recibido una carta tradicional remitida a nuestro nombre y con nuestra dirección, y al abrirla nos encontramos con una misiva muy conceptuosa de un banco, financiera o casa comercial, con la cual no mantenemos ninguna relación comercial, comunicándonos la grata sorpresa que tenemos aprobado un crédito por una suma nada de despreciable. Posiblemente, todos al recibirla nos decimos, que bueno y pensamos inmediatamente que objetivo darle a ese dinero, que se me ofrece en condiciones tan ventajosas y de manera tan oportuna. Pero quienes realmente se sientan a pensar, quien le entrego mis datos a dicha institución?, que otros datos más mantendrán de mi persona y mi familia?, etc. Simples hechos como los señalados, demuestran que no conocemos nuestros Derechos Constitucionales, ya que durante muchos años estaba en desuso o sencillamente no era el tema; pero ello mismo, nos lleva a otro problema, el cual no es directamente parte de este trabajo, ¿debe el Estado educar a las personas a vivir en este mundo digital, o simplemente su intervención debe ser desde la regulación y legislatura?.
Tal como señalamos anteriormente, debemos lograr desentrañar que es lo que queremos sancionar o legislar, a donde debemos apuntar.

En tal orden de cosas, queda claro que debemos lograr en principio determinar o definir los llamados **“contenidos prohibidos”**; es decir, que es lo que sancionaremos, y que características mínimas debe presentar.

Para ello debemos fijar nuestra atención en elementos como la masividad, el propósito, la forma del envío, la obtención de las direcciones de casillas

electrónicas y la veracidad del mensaje.

En cuanto a la masividad, la comunicación enviada podrá ser considerada Spam, sólo si se envía a determinado número de usuarios, es decir, si a mi un sujeto me envía comunicaciones comerciales no solicitadas por mi, y me la envía sólo a mi, podría ser sancionado?

Otro punto a determinar es el propósito o fin de la comunicación. Sólo podré reclamar si contiene un contenido comercial o publicitario de algún producto o servicio que yo no haya solicitado?, o podré sentirme afectado y solicitar la protección legal para hacer valer mis derechos, ante comunicaciones que compartan conmigo ideologías políticas o religiosas? O aquellas que me invitan a ser miembro de un sindicato o federación de sindicatos? O incluso aquellas que me invitan día a día a salvar mi alma descarriada a través de la lectura de la Biblia u otros textos sacros?

Al respecto podemos citar ejemplos entregados en un estudio elaborado por la **INTERNATIONAL TELECOMMUNICATION UNION (ITU)** [48] el año 2005. En ella se señala que ***"The initial decision for regulators in assessing spam is whether to differentiate among messages based on their content or purpose. Many spam laws focus on messages that have a commercial purpose; they seek to advertise a product or service to the recipient.",*** es decir, hay que atender a si el mensaje tiene por objeto un propósito comercial; intentando promocionar un producto o un servicio al receptor del mensaje. Este mismo informe cita como ejemplo las leyes japonesas de Spam, las cuales sólo se aplican al caso que sean comunicaciones enviadas por empresas u organizaciones que le envían comunicaciones a personas que hayan contratado con ellas en alguna

48 ITU. A comparative analysis of spam laws: The quest for a model law. [en línea] [Fecha de consulta: 11 marzo 2007] Actualización permanente. Disponible en http://www.itu.int/home/index.html.

oportunidad, con lo cual el concepto mayoritario de correo masivo no deseado no encuentra aplicación acá.

El mismo informe anterior, pone como ejemplo la contradicción entre la Ley Norteamericana en la materia frente a la Ley Australiana, en que las comunicaciones políticas no solicitadas se encuentran prohibidas por la Constitución Americana, en cambio las leyes Australianas las permiten precisamente en resguardo del Derecho Constitucional de las comunicaciones políticas[49].

Otro asunto a considerar es la forma o método del envío del mensaje. La ley deberá apuntar sólo a los mensajes enviados vía email? O considerara los mensajes a través de los servicios de mensajería instantánea como Windows Messenger, Yahoo Messenger, Skipe, etc? o los mensajes publicitarios que se envían a través de los sistemas de mensajería de texto o voz en teléfonos móviles? E incluso las llamadas de audiotexto automática que recibimos vía telefónica tradicional, y que son muy comunes en época de elecciones políticas, invitándonos los múltiples candidatos que nos debieran interesar, a confiar en ellos y entregarles nuestra voto en las elecciones venideras?. Y que pasa al navegar por la web y intentar abrir una página de nuestro interés nos encontramos con los llamados **POP-UP's**[50], que mas allá de que pueden contener información indeseable, pueden invitarnos a acceder a miles de productos o servicios? Etc, ¿acaso no estamos frente al mismo problema de fondo?

En este escenario se cita los casos de algunas leyes Anti-Spam, por ejemplo la **Directiva 2002/58 de la Comisión de las Comunidades Europeas (CCE**) se aplica todos los métodos de comunicación electrónica,

49 ITU. A comparative analysis of spam laws: The quest for a model law. [en línea] [Fecha de consulta: 11 marzo 2007] Actualización permanente. Disponible en http://www.itu.int/home/index.html.
50 Nueva ventana del programa navegador, generalmente de tamaño reducido a escala de la ventana principal, que aparece cuando el usuario está descargando un página determinada.

en Estados Unidos se refiere solamente al correo electrónico y, por ejemplo, las comunicaciones por SMS son reguladas independientemente. En este caso debemos recordar los proyectos del Senador Jaime Naranjo y del Senador Carlos Ominami, ya citados con anterioridad en este trabajo, que buscan regular las comunicaciones no solicitadas por vía telefónicas.

Un punto interesante a resolver en el futuro, será lo que ocurrirá una vez que este en absoluta vigencia la llamada Telefonía sobre IP, ya que necesariamente se entremezclara su actuar con la telefonía tradicional local y móvil. Al respecto se señala en el referido informe de la ITU que se deberá buscar y determinar que elementos se aplicaran a uno u otros sistema y cuales deberán aplicarse en común.[51]

Por otra parte, sólo podrían sancionar a quienes efectivamente hayan obtenido nuestros datos de manera ilegitima? Es decir, que ocurre con aquellos programas del tipo **RATWARE**[52] o **SPAMBOTS**[53], que una vez encontrado un servidor, sencillamente a través de un sistema automático, algorítmico y de combinación de letras comienza a enviar emails a direcciones desconocidas, jugando en un sistema de prueba y error o acierto? O en el caso de las comunicaciones telefónicas una máquina selecciona una serie de números telefónicos existentes, sin conocer sus titulares y comienza automáticamente a llamar a personas indeterminadas? O qué ocurre con aquellos remitentes que toman sencillamente los datos que hemos entregado en la red para otros fines, pero que se encuentran libremente en ella, y que normalmente se accede a

51 "Indeed, the advent and growing popularity of Voice over Internet Protocol (VoIP) for telephony will likely confront regulators dealing with unsolicited communications with the convergence of IP-based systems, such as the Internet and circuit-routed systems (e.g. standard telephone service). Thus, specifying the media to which a regulation applies is common, but the choice of media to cover varies from system to system."
52 Software que usan los spammers para automatizar campañas de spam, coordinar servicios de spam y generar, enviar y monitorizar mensajes de spam.
53 Programa que utilizan los spammers para recolectar direcciones electrónicas desde Internet.

ellos a través de programas de recolección[54]? O lo que ocurre a través del las llamadas **WEBMINING**[55] que nos ofertan en base a nuestros gustos o preferencias de navegación en la red?

Al respecto en la mayoría de las legislaciones se establecen prohibiciones a recolectar casillas de Correo electrónico y otros datos de contacto en la red. Básicamente se mencionan dos problemas en este asunto.

El primero es la llamada práctica "**ADDRESS HARVESTING**" o cosecha de direcciones. Es válido para los emisores buscar en la red, incluyendo expresamente páginas Web, blogs, ChatRooms, y grupos de las noticias; localizar y compilar direcciones del E-mail. En los Estados Unidos, la llamada CAN-SPAM Act of 2003, por ejemplo, se prohíbe enviar de E-mail comercial a los receptores de direcciones que fueron obtenidas por un medio automatizado, ya que estas no fueron entregadas con dicho fin[56]. Por su parte la CEE por medio de la Directiva 95/46 prohíbe esta cosecha tanto si ha sido hecha manualmente o vía las herramientas del software.

En Chile nada hay dicho, pese a que en el proyecto de ley[57] patrocinado por el Senador **Jovino Novoa** el año 2005, que pretendía elevar las

---

54 Programa que examina páginas Web y filtra mensajes de listas de correo para obtener direcciones de email a las que enviar spam

55 Técnicas que ayudan a descubrir patrones de la actividad de los usuarios cuando acceden a los sitios web. Permiten ajustar actividades como el marketing on-line, la selección de banners o interstitials publicitarios, segmentación de usuarios y gestión de relaciones con clientes. Manejan, con el soporte de bases de datos específicas, un gran volumen de datos sobre accesos a páginas web y datos de clickstream.

56 (d) PROHIBITION OF TRANSMISSION OF CERTAIN COMMERCIAL ELECTRONIC MAIL FROM ILLEGALLY HARVESTED ELECTRONIC MAIL ADDRESSES- (1) IN GENERAL- No person may initiate in or affecting interstate commerce the transmission, to a covered computer, of a commercial electronic mail message that is prohibited under subsection (a), (b), or (c), or assist in the origination of such a message through the provision or selection of electronic mail addresses to which the transmission of such message is initiated, if-- (A) the electronic mail address of the recipient was obtained, using an automated means, from an Internet website or proprietary online service operated by another person; and (B) the website or proprietary online service from which the address was obtained included, at the time the address was obtained, a notice stating that the operator of such a website or proprietary online service will not give, sell, or otherwise transfer addresses maintained by such site or service to any other party for the purpose of initiating, or enabling others to initiate, commercial electronic mail messages.

57 Proyecto de Ley, que busca modificar la ley nº 19.628 en lo que se refiere a la publicación de boletines con información de datos personales-patrimoniales, con el objeto de proteger mas adecuadamente los derechos de las personas y de las pymes. además, propone modificar la ley para dar una mejor protección a los "datos sensibles" y hacerse cargo de los problemas derivados del "Spam".

direcciones de correo electrónico al carácter de datos personales sensibles, establecía en su articulado que debía entenderse por fuente pública de datos, y sin que se excluyera como tal las direcciones de correo publicadas en sitios web. Además agregaba en el artículo 9 que ***"Los datos personales a que alude la presente ley deben utilizarse para los fines considerados o declarados por sus titulares al momento de su comunicación, registro o almacenamiento, salvo que provengan o se hayan recolectado de fuentes accesibles al público. Respecto a la recopilación de datos personales de empresas o personas naturales, obtenidos directamente de sitios de la red Internet, de manera alguna podrá entenderse que ha sido otorgada una autorización tácita para su uso con fines diversos a los inherentes a los derivados de la naturaleza o finalidad del sitio".*** En la legislación Argentina encontramos las misma prohibición, siempre y cuando el titular no haya colocado su información en un sitio web público, ya que en dicho país es uno de los pocos lugares que le ha dado a la dirección de correo electrónico el carácter de dato sensible personal[58].

El otro problema de especial consideración en este tema son los llamados "**DICTIONARY ATTACKS**" o "**ATAQUES DE DICCIONARIO**" que es una herramienta muy común utilizada por los spammers, que por medios automáticos empleando algoritmos generan direcciones de E-mail, combinando letras y números para formar probables direcciones; por ejemplo, un remitente sabe que existe la extensión de @chile.cl y construyo una lista de dirección alimentada con los apellidos y nombres de uso

58 Ley 25.326. Protección de los Datos Personales. Artículo 5. (Consentimiento).
1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.
El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6º de la presente ley.
2. No será necesario el consentimiento cuando:
a) Los datos se obtengan de fuentes de acceso público irrestricto;...

frecuente en el país. La operatoria consiste en que una vez que esos mensajes no rebotan o que el usuario les devuelve una denegatoria, ellos sencillamente han validado la existencia de dichas direcciones, las cuales podrán ser blanco de ellos mismos, o de terceros a quienes ellos vendan dichas bases de datos. Corea del sur en la ya citada ley, prohíbe utilizar cualquier programa que cree la información receptora del contacto, tales como direcciones de E-mail o números de teléfono, combinando letras, marcas, y números.[59] Igual prohibición establece Japón.[60]

Sin duda, el objetivo de estas prohibiciones no es más que poner mayores trabas a los spammers, ya que tendrán limitaciones para crear bases de datos y además será mas difícil la compra de las mismas.

Por otra parte, hay que preguntarse si importa si el mensaje y su contenido, así como su remitente son auténticos, dejando de lado la situación de un eventual fraude penal?.

Al respecto hay que señalar, que la mayoría de los países y sin entrar a detenernos en el concepto u extensión del Spam, prohíben los mensajes con contenido fraudulento, falso o que inducen al engaño o error del receptor, incluyéndose en estas categorías las que falsean la identidad o dirección de email del remitente, las que en la etiqueta o contenido del asunto del mensaje no dice nada o dan otra información, o aquellos que al contestarlos el receptor, solicitando que no se le envíen mas mensajes rebotan y no son recibidos. Incluso en estos casos se utilizan, técnicas que afectan a terceros inocentes, como cuando la dirección de envío es falsa y corresponde a alguien que no tiene ninguna responsabilidad en la

59 ITU. A comparative analysis of spam laws: The quest for a model law. [en línea] [Fecha de consulta: 11 marzo 2007] Actualización permanente. Disponible en http://www.itu.int/home/index.html
60 ITU. A comparative analysis of spam laws: The quest for a model law. [en línea] [Fecha de consulta: 11 marzo 2007] Actualización permanente. Disponible en http://www.itu.int/home/index.html

cuestión, y se ve incluso afectado, por un verdadero bombardeo de emails rechazando las supuestas comunicaciones electrónicas no deseadas que habría realizado, y en algunos casos en su reputación, como le ha ocurrido a muchísimos bancos y proveedores como **Amazon** a raíz de las acciones Phishing.

Como es de imaginar, estas prohibiciones se superponen con otras leyes que prohíben o sancionan criminalmente los fraudes. Al respecto se cita[61] como ejemplo la legislación de la CEE que trata la publicidad fraudulenta o engañosa en la Directiva 84/450/CEE,. Por su parte Perú prohíbe el uso de una identidad falsa en mensajes del E-mail y la falsificación de datos en su Código Penal.

Todos estos temas en busca de determinar los contenidos prohibidos son sin duda el primer escalón para abordar este problema.

Supongamos fictamente, que hemos pasado ese primer escalón, habrá que analizar qué tipo de legislación nos daremos, una especial? Que regule exclusivamente el Spam y demás comunicaciones no deseadas? Sólo en el ambiente Internet o se incorporará las otras formas de comunicación? O quizás bastará con adecuar otras leyes vigentes, como la ley de telecomunicaciones, leyes de defensa del consumidor, o modificar expresamente la Constitución Política de los países, etc.

Por otra parte en este desentrañamiento de problemas, que ocurrirá con la adopción de sistemas para prevenir el Spam, es decir, que reglas o normas deben respetar (si es que partimos de la ilusión que hay un interés en

[61] ITU. A comparative analysis of spam laws: The quest for a model law. [en línea] [Fecha de consulta: 11 marzo 2007] Actualización permanente. Disponible en http://www.itu.int/home/index.html

respetarlas) quienes envían las comunicaciones?. Con esto nos estamos refiriendo al hecho de que si los remitentes pueden entrar en contacto conmigo sin mi permiso anticipado, es decir, que pasara si mi sistema se rige por el Opt-In o Opt-Out ya definidos en este trabajo, y que apuntan al hecho de que los reguladores como cuestión inicial, determinen si los mensajes no solicitados están permitidos o prohibidos.

Si dichos mensajes se permiten, tal como se señalo en la introducción técnica de este trabajo, estamos frente a un sistema Opt-Out, por el contrario si se encuentra prohibido estamos frente a un sistema Opt-In.

Este tema no es menor, a la hora de establecer una legislación adecuada, ya que si optamos por un sistema Opt-In, esta deberá detenerse especialmente en la forma obtención de las direcciones de correo electrónico, en su almacenamiento y tratamiento de conformidad a sus leyes de protección de datos, si es que existen. Si se ha optado por un sistema Opt-Out, lo primordial será establecer las formas en que el receptor deberá hacer presente su voluntad de no recibir mensajes, y que medidas deberán tomar los remitentes para respetar esta voluntad.

En este punto encontramos una gran confrontación entre diversos regimenes legales internacionales respecto al Spam. En efecto, en Estados Unidos, Corea del sur, y Colombia se emplea el sistema Opt-Out, por consiguiente permite que personas naturales o jurídicas envíen comunicaciones no solicitadas. En cambio, por su parte Australia y la Unión Europea han adoptado el sistema Opt-In, lo cual implica la prohibición a los remitentes de enviar comunicaciones a los receptores que no las hayan solicitado expresamente, como ocurre hoy día con las acciones de email marketing que analizábamos en otro acápite de este capitulo.

Este punto es señalado por el documento de la ITU ya citado, como un punto donde debe encontrarse armonización, y por ello abogan por una ley modelo respecto del Spam, ya que este punto coloca a dos países en absoluta contradicción, ya que mientras en uno el envío es permitido en el otro se está transgrediendo la legislación.

Al respecto también existen excepciones, o métodos híbridos o llamados de sistema "**SOFT OPT-IN**", en virtud del cual si un receptor en algún momento me solicitó información de tal o cual producto, yo me encuentro habilitado para enviarle información de otros, siempre y cuando pueda manifestar mi consentimiento tardío de no seguir recibiendo tales comunicaciones, como se permite en el Reino Unido[62] o Malta[63].

El llamado "**Soft Opt-In**" requiere por parte de los Estados miembros de la CEE de conformidad a la Directiva 2002/58 para que opere esta excepción es que el consumidor haya indicado anteriormente interés en este tipo de transacciones comerciales y que haya dado el consentimiento para recibir

62 The Privacy and Electronic Communications 2426.(Use of electronic mail for direct marketing purposes. § 22. - (1) This regulation applies to the transmission of unsolicited communications by means of electronic mail to individual subscribers. (2) Except in the circumstances referred to in paragraph (3), a person shall neither transmit, nor instigate the transmission of, unsolicited communications for the purposes of direct marketing by means of electronic mail unless the recipient of the electronic mail has previously notified the sender that he consents for the time being to such communications being sent by, or at the instigation of, the sender. (3) A person may send or instigate the sending of electronic mail for the purposes of direct marketing where – (a) that person has obtained the contact details of the recipient of that electronic mail in the course of the sale or negotiations for the sale of a product or service to that recipient;(b) the direct marketing is in respect of that person's similar products and services only; and (c) the recipient has been given a simple means of refusing (free of charge except for the costs of the transmission of the refusal) the use of his contact details for the purposes of such direct marketing, at the time that the details were initially collected, and, where he did not initially refuse the use of the details, at the time of each subsequent communication. (4) A subscriber shall not permit his line to be used in contravention of paragraph (2).) http://www.opsi.gov.uk/si/si2003/20032426.htm.

63 Processing of Personal Data (Electronic Communications Sector) Regulations, 2003 (under the Data Protection Act (CAP. 440), L.N. 16 of 2003)(Regulation 10 of such legal notice relates to the use of publicly available electronic communication services to send unsolicited communications for the purpose of direct marketing by means of an automatic calling machine, e-mail or fax. The regulation provides that such communication cannot be sent unless: 1. the subscriber has given his prior explicit consent in writing to the receipt of such communication; or 2. the person/organisation has obtained from his customers their contact details for electronic mail in relation to the sale of a product or service. In this case such person/organisation may use such details for direct marketing of its own similar products or services. In any case, customers shall be given the opportunity to object free of charge, and this in an easy and simple manner. Also, communication for direct marketing purposes disguising or concealing the identity of the sender or without a valid address, to which the recipient could send a request that such communications cease, is prohibited. Any person who fails to comply with the aforesaid, shall be liable to an administrative fine, not exceeding Lm10,000, which fine shall be determined and imposed by the Data Protection Commissioner.) http://www.dataprotection.gov.mt/article.aspx?art=154

comunicaciones adicionales y similares.

Por último y en otro orden de cosas, debe establecerse un sistema de comunicaciones con etiquetado?, como hace la ley de protección de derechos de los consumidores en Chile y varias otras en el mundo. Es decir, debe establecerse la obligación de que el asunto o subject del mensaje se indique el objetivo del mismo. Que se indique o se individualice correctamente al emisor del mensaje.

Por ejemplo, Corea del sur en la **"ACT ON PROMOTION OF INFORMATION AND COMMUNICATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION OF 2001**"[64] requiere que el emisor incluya el contenido objetivo y principal del mensaje, su nombre y dirección o número de teléfono, la fuente de la cual obtuvo la dirección del E-mail del receptor, e instrucciones para otorgar su declaración de no recibir mas mensajes en el futuro. Por su parte en México en la **LEY FEDERAL DE PROTECCIÓN DE LOS CONSUMIDORES**, en el artículo 17[65], se establece la obligación de que los emisores incluyan su nombre, dirección, y número de teléfono, junto con los del negocio a nombre de el cual se envía el mensaje y también la información sobre la oficina del abogado federal para la protección al consumidor.

Por su parte, en Chile, el legislador estableció en una modificación a la **LEY DE DEFENSA DEL CONSUMIDOR Nº 19.496**, en su artículo 28 B un

---

64 Citado. ITU. A comparative analysis of spam laws: The quest for a model law. http://www.itu.int/home/index.html

65 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. http://www.mexicolegal.com.mx/m_help.htm

sistema similar al señalar ***"Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos.***

Los proveedores que dirijan comunicaciones promociónales o publicitarias a los consumidores por medio de correo postal, fax, llamados o servicios de mensajería telefónicos, deberán indicar una forma expedita en que los destinatarios podrán solicitar la suspensión de las mismas. Solicitada ésta, el envío de nuevas comunicaciones quedará prohibido."

El ya mencionado proyecto de los Senadores Ominami y Naranjo, contienen en un articulado propuesto, en especifico el artículo 34 B una descripción mas completa que la contenida en la normativa vigente, de las exigencias que deben contener los correos electrónicos comerciales o publicitarios para ser considerados como validos o legitimos. En efecto se señala en la referida norma ***"El Correo Electrónico Comercial o publicitario deberá contener y exhibir de forma sencilla, clara y completa:***

a) Una descripción breve, precisa y representativa del contenido del correo electrónico y la palabra "publicidad"; "anuncios"; "circulares"; "ofrecimiento"; "propuesta"; o "invitación", en el campo del objeto o asunto

b) Datos de identificación del emisor, incluyendo nombre y apellido o razón social, domicilio físico, teléfono y dirección de correo

electrónico, así como iguales menciones respecto del proveedor de bienes o prestador de servicios por cuyo encargo se inicia la transmisión del mensaje, cuando se trate de una persona distinta del remitente.
Se entenderá por emisor a la persona quien inicia un mensaje y cuyo producto, servicio o sitio de INTERNET es anunciado o promocionado por el mensaje.

c) Un vínculo o una dirección de correo electrónico válida a la que el destinatario pueda solicitar, expedita y gratuitamente, la suspensión de los envíos, que quedarán desde entonces prohibidos. Dicho vínculo o dirección deberá mantenerse vigente por, al menos, 30 días después de haberse enviado el mensaje; y

d) Tratándose de publicidad o anuncio de productos y servicios para mayores de edad, las comunicaciones respectivas sólo podrán ser enviadas a destinatarios que hayan prestado consentimiento previo de manera expresa de conformidad con lo dispuesto en el artículo 34 A. En estos casos, el proveedor de bienes o servicios deberá implementar y aplicar sistemas, dispositivos o mecanismos idóneos para constatar que el destinatario que ha prestado su aceptación, es mayor de edad. Tales mensajes deberán incluir en la sección "asunto" la frase "PUBLICIDAD PARA MAYORES DE EDAD".[66]

Obviamente estas exigencias tienen variados objetivos. Se señalan fines de toma de conciencia, responsabilidad, regulación y filtración o contenido. Se dice que ayudan a la toma de conciencia, por cuanto los receptores, adquieren la conciencia o el conocimiento de quien efectivamente está

[66] BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 6136-03. [en línea] Chile. [Fecha de consulta: 30 Noviembre 2008] Actualización permanente. Disponible en: http://www.bcn.cl/

enviando una comunicación electrónica. Por otra parte, ayudan a la responsabilidad, por cuanto el emisor debe identificarse, y por lo tanto se ve obligado a resguardar su reputación. También se dice que ayuda a la regulación, pues al conocerse todos estos datos, se pueden predeterminar a acciones a seguir, para el caso de que se fuera de las manos la situación. Y por último ayuda al bloqueo, ya que el usuario puede establecer criterios en su equipo para filtrar o bloquear mensajes enviados con tales o cuales características o contenidos.

Cuando nos referimos a que los mensajes sean etiquetados, estamos hablando de un sistema que permita a los usuarios o receptores identificar a ellos o a los filtros que tenga instalados en su equipo que mensajes son Spam o correos electrónicos no deseados. Así por ejemplo podemos citar que Corea del sur por disposición legal los mensajes de publicidad contienen el carácter "@" en el asunto o subject, en los Estados Unidos los caracteres ***"ADV"*** y en España la expresión ***"publicidad".*** En el mismo sentido en Chile, en el proyecto de ley recién citado, se establece la obligación de incorporar en el asunto las palabras ***"publicidad"; "anuncios"; "circulares"; "ofrecimiento"; "propuesta"; o "invitación"*** asi como la obligación de señalar que es para adultos, cuando ese sea el objetivo.

Otro tema de la mano con las llamadas etiquetas o indicación del contenido, viene dado por la opción de "***darse de baja***" o solicitar la eliminación de la lista, a fin de que el emisor me retire de su base de datos, y pueda manifestar mi voluntad válida de no recibir más mensajes no solicitados, requisito que es de suma importancia en los sistemas OPT-OUT ya mencionado, puesto que proporciona los medios por los cuales los receptores controlan si reciben o no mensajes comerciales. En el otro sistema es igualmente importante, cuando el receptor desea cambiar de

opinión respecto a la recepción de mensajes comerciales.

Al respecto la legislación no es uniforme, en la forma de operar las "dadas de baja", puesto que algunas les basta que el mail contenga los datos para hacerlo, tales como ingresando a determinada pagina web o llamando a un determinado teléfono, o enviando un email a una dirección determinada. En Australia se requiere que los remitentes proporcionen una funcionalidad Opt-Out, usando la misma tecnología con la cual el mensaje fue enviado, es decir, si el mensaje fue enviado por email, se le debe dar la facilidad al emisor de dar su baja vía email.

Otras características en estas leyes serán los plazos para que quede operativo la baja o el idioma en que debe hacerse, así por ejemplo, no se avanzaría mucho si en el email o mensaje se señala para un hispano parlante se pueda dar de baja, se escribiera o se le hablara en Chino.

Un único problema que trae aparejado este sistema de tener que solicitar la baja, es que es un método utilizado por los spammers para validar la existencia y vigencia de la dirección de correo electrónico, lo que trae como consecuencia muchas veces que comienzan a llegar más Spam.

Sigamos avanzando, e imaginémonos que logramos solucionar todos los problemas anteriores, surge el último y quizás el más difícil de todos, como, cuando y quienes van a ser los encargados de hacer cumplir con dichas leyes o regulaciones. Quien o quienes van a sufrir los costos de hacer cumplir dichas regulaciones; que papel va a tomar el estado en ello, que va a ocurrir con los privados que proveen estos servicios y con los usuarios de los mismos?

En primer lugar, quien será el responsable de aplicar estas leyes o hacerlas cumplir. Que pasa si una comunicación involucra a dos países,?,

es decir en que el remitente y receptor pertenezcan a dos jurisdicciones distintas.

Normalmente, se persiguen los delitos e ilícitos que se cometen dentro de nuestras fronteras, razón por la cual email enviado desde el extranjero nos impediría su persecución real, con lo cual la ley existente perdería toda su eficacia.

Si bien, no muchos aceptan la extraterritorialidad, existen algunos como Australia[67], que considerara siempre como un Spam regido por sus leyes y dentro de su jurisdicción, si se dan alguna de las siguientes situaciones:

1. el mensaje se origina en Australia
2. el individuo que envió o autorizó el envío del mensaje se encontraba en Australia cuando se envía el mensaje, o la organización que envió o autorizó el mensaje tiene o tenía la sede principal de sus operaciones en Australia al momento del envío.
3. El mensaje fue recibido en un computador que se encuentra en Australia
4. el ESP, es de origen australiano o
5. si el mensaje no podía ser entregado por cuanto no existía la dirección de correo receptora, es razonablemente presumible, que dicha comunicación llegue a una computadora o un servidor en Australia.

En el caso antes descrito, encontramos que un Spam prácticamente podrá ser perseguido en Australia de acuerdo a sus leyes, pues la posibilidad de que este en alguna de esas situaciones es muy alta, más allá de que logre

[67] Dana. Centro de conocimientos. Reglamentos, Leyes y Legislaciones Antispam en el mundo [en línea] Spam Act 2003 [Fecha de consulta: 11 marzo 2007] Actualización permanente. Disponible en: http://www.danacrm.com/wiki/images/d/df/SPAM_ACT_2003.pdf

sancionar o ejecutar al spammer en si.

La extraterritorialidad, como problema no es para nada simple, por cuanto tal como señalamos en otro acápite, lo que para un país es Spam para otro no, tal como ocurre con el tema del OPT-OUT y el OPT-IN. Obviamente una ley puede obligar válidamente a sus nacionales dentro de su territorio, pero que ocurre con los agentes que operen fuera de sus fronteras. Así, la legislación del Spam pudo cubrir las acciones del ciudadano de un estado mientras que ella estaba fuera de sus fronteras. Australia, por ejemplo, especifica que su ley se extiende a los actos y omisiones aun fuera del país. España por su parte exige jurisdicción sobre personas y organizaciones, aun fuera de sus límites y de la Comunidad Europea, si las acciones ocurridas amenazan el orden público, e incluye expresamente el Spam.

Si bien puede ser beneficiosa la extraterritorialidad de las leyes de Spam, puede generar conflictos entre los distintos países, pues se estarían vulnerando las soberanías, si no existen acuerdos al respecto.

Uno de los métodos más comunes es la utilización de los llamados "**MOU**", en virtud de los cuales los países y sus organismos competentes en estas materias, suscriben acuerdos de cooperación entre ellos, de manera de poder salvar las diferencias de jurisdicción existentes. Por ejemplo la UE ha propuesto regulaciones con fuerza ejecutiva a fin de proteger a los consumidores, entendiéndose incorporados en ese escenario los Spams.

Por otra parte hay que dilucidar, quien será el responsable de la vigilancia, control y sanción. Una autoridad de control de datos como ocurre en España o supuestamente en la Argentina. Un organismo dependiente por ejemplo del Ministerio de Transportes y Telecomunicaciones o de otra cartera de gobierno como podría ocurrir el día de mañana en Chile, o

simplemente los Tribunales de Justicia.

Sin duda la aplicación y control de la ley y su respeto es uno de los temas más críticos para el correcto diseño de una ley armónica al respecto; pues una ley perfecta en el fondo, que prevea todas las hipótesis, pero que carezca de los procedimientos y responsables de su respeto, puede significar un esfuerzo fatuo e inútil; presentándose situaciones como lo que ocurre en Chile, con la ley Nº 19.628, sobre Protección de la vida privada, en que carece de una autoridad de control, contrariamente a lo que ocurre en otros entornos en que si ha tenido una adecuada aplicación. De que sirve una ley que no se pueda aplicar, de nada, y quizás sea hasta un incentivo para que spammers de todo el mundo, busquen esa jurisdicción para establecer verdaderos carteles o paraísos del Spam mundial.

Por otra parte muchos países, al dictar una ley de Spam perfecta o modelo, se enfrentaran al hecho de que más de una autoridad pueda conocer del asunto. Muchos regímenes enfrentarán la posibilidad de entidades múltiples para las cuales sea potencialmente competente o cargado con la regulación del Spam.

Ahora, que ocurrirá cuando dicha comunicación no deseada, no sólo sea eso, sino que además traiga aparejada la comisión de delitos, como podría ser un ACE de Phishing. Que autoridad tendrá competencia y cual deberá inhibirse de ella? Qué ley se aplicará en caso que dicha comunicación afecte por ejemplo la ley de Defensa del Consumidor, el Código Penal y la eventual legislación de Spam?

Un punto no menor, es determinar la extensión de la responsabilidad. Será sólo responsable el remitente del Spam? o podrá ser también el ISP o ESP

respectivos? No hay que olvidar, que en relación a los contenidos de Internet, han aparecido algunos que han pretendido que los ISP respondan por las expresiones, informaciones y contenidos en general que se publican en la red, casi como haciendo aplicable las normas de la ley de prensa a la imprenta donde se imprime un periódico. Incluso también podría serlo el fabricante del software creado para enviar las comunicaciones e incluso el autor del software cliente de correo que utilizan los usuarios. Y es más, tratándose de Spam internacionales, que pasa con la responsabilidad de los distintos Estados. No hay que olvidar, que a través de Tratados Internacionales (por ejemplo los llamados TLC) y de convenios, se han establecido ciertas obligaciones, de manera de poder asegurar por un parte el respeto a los Derechos de Propiedad Intelectual (muy vulnerados a través de los emails y la red en general) o la protección de los datos privados de las personas en las trasmisiones internacionales.

En efecto, una característica de las leyes AntiSpam es quien será sancionado o perseguido por el Spam. La respuesta puede aparecer de entrada como muy simple, el **REMITENTE**, pero existen una serie de agentes adicionales que de una u otra manera incentivan o se benefician con este ilícito. En ese escenario, la empresa que contrata a un spammer para publicitarse, si bien no comete el ilícito debiera ser sancionada al igual que si las comunicaciones no solicitadas las hubiera enviado ella, con una especie de responsabilidad subsidiaria. La razón es muy simple, estas organizaciones o empresas, están abusando de un sistema de publicidad que les trae aparejado costos muy bajos, pero les puede generar muchos ingresos, aun con tasas de retorno bajísimas, generándose un Enriquecimiento injusto y el consiguiente empobrecimiento del dueño de los servidores, del ISP o del ESP, que soportan estos caudales de correo basura, y con tal de que no se dañe su servicio, invierten en herramientas computacionales de alto costo, tales como filtros y sistemas de listas de bloqueo (black list), etc.

En este sentido podemos citar el caso australiano, donde se prohíbe el envió de correos no solicitados e impone responsabilidad a toda persona que ayude, induzca, o conspire para la realización de tal actividad[68].

Situación semejante pretende sancionar Singapur, pues en un proyecto de ley denominado **"FRAMEWORK FOR THE CONTROL OF E-MAIL SPAM"** se establece que el comerciante que directamente o a través de comisionista incentiva o procura el Spam también es obligado a las sanciones del Spam.[69]

Otro factor importante respecto a la responsabilidad en torno al Spam, es eximir a los ISP y ESP por la instalación de filtros o bloqueos, ya que hay que tener en claro que ello, implica una violación a la privacidad de las comunicaciones.

En Corea del sur se autoriza a los ISPs a establecer bloqueos, siempre y cuando sean notificado a los clientes y autorizados por estos en los contratos que los vinculan con el ISp o ESp en su caso.

Por otra parte existe, el problema que estos filtros o bloqueos pueden eliminar o detener comunicaciones validas, que sean identificadas erróneamente como spam.

Obviamente el establecer estos filtros por parte de las empresas, puede constituir ventajas comparativas a la hora de competir con otros

68 ITU. A comparative analysis of spam laws: The quest for a model law. [en línea] [Fecha de consulta: 11 marzo 2007] Actualización permanente. Disponible en http://www.itu.int/home/index.html
69 ITU. A comparative analysis of spam laws: The quest for a model law. [en línea] [Fecha de consulta: 11 marzo 2007] Actualización permanente. Disponible en http://www.itu.int/home/index.html

proveedores, y podría significar incluso el establecimiento de tarifas diferenciadas.

Finalmente, es importante atender a las penas y sanciones. Que penas se establecerán? Simples multas o penas pecuniarias, prohibiciones de operar, sanciones penales, etc? Que ocurrirá con la reincidencia de estas acciones, se aplicarán normas de eximentes de responsabilidad penal, operará la prescripción, etc, es decir, se someterán al régimen normal del derecho de un país?

Estas penas normalmente serán penas administrativas, indemnizaciones de perjuicios civiles y penas privativas de libertad.

Las primeras quizás sean las que menos importen, ya que dependiendo del monto de las multas establecidas, ellas normalmente serán mucho menores que las ganancias que se pueden obtener en este negocio.

En cuanto a las indemnizaciones civiles, obviamente pueden ser más amenazantes para los spammers, pero será necesariamente el afectado quien deba llevar todo el desgaste a fin de obtener una condena que le resarza de los perjuicios.

Por último, si atendemos a penas de cárcel o privativas de libertad, debiera ser el Estado quien moviera dicha procedimiento, de manera que el afectado no se sienta disminuido o limitado por tener que afrontar dicho esfuerzo, y que posiblemente por tratarse de negocios al margen de la ley, y de autenticas mafias, los denunciados no escatimarán en gastos en pro de su defensa.

Al respecto el informe ITU, señala una serie de ejemplos. Señala que en México se establecen multas de conformidad a la Ley Federal de Protección

al Consumidor, para aquellas violaciones. Estas multas van en aumento, por las reiteraciones y con llevan penas de cárcel en casos extremos. Por su parte, en Corea del sur crea responsabilidad civil hasta por diez millones de wones para la mayoría de las violaciones de sus leyes anti-Spam y también establece penas criminales para los spammers que envían anuncios de contenido adulto a menores de edad o que utilizan herramientas tecnológicas prohibidas.

El nivel y el tipo de penas es uno de los puntos, pues sería deseable la correspondencia entre los países, de manera que no existieran países que corrieran el riesgo de verse infectado de estos noveles empresarios, o que les permitiera crear su paraíso del ACE.

4.- Problemática jurídico constitucional en torno a una ley Anti Spam

Previo a finalizar este capítulo y también relacionado con los problemas del Spam y su eventual regulación, hay que atender a la problemática que se puede presentar ante una ley antispam, dictada sin observar el panorama completo del ordenamiento jurídico de un país.

En efecto, son innumerables los autores y profesores, que al referirse a los llamados Principios básicos del Derecho Informático, nos estamos refiriendo exclusivamente a la concreción de las Garantías fundamentales de todas las personas, en el mundo de las llamadas **TIC'**s.

En efecto, antes de decidir al respecto, es de suma importancia que los legisladores y reguladores, tengan claro, la relevancia de los siguientes principios:

1.- La Neutralidad Tecnológica
2.- La equivalencia funcional;
3.- La equivalencia normativa; y
4.- El principio de mínima intervención.

Estos principios que analizaremos a continuación, son de suma importancia a la hora de legislar sobre materias tan delicadas, como pretende hacerse a través de la moción en comento.

A.- La Neutralidad Tecnológica

Podemos partir definiendo la "**NEUTRALIDAD TECNOLÓGICA**" como la "***Propiedad de un sistema de información en virtud de la cual el acceso al sistema o a los datos contenidos en él no está condicionado al empleo de determinadas plataformas tecnológicas***". La neutralidad tecnológica se logra, esencialmente, mediante el apego a estándares abiertos, tales como los fijados por la **INTERNATIONAL STANDARDS ORGANIZATION** (ISO) o por el **WORLD WIDE WEB CONSORTIUM** (W3C) para la web.

En virtud de este principio los poderes del Estado, deben actuar de determinada manera, a fin de que se mantenga dicha garantía.

En lo respecta al poder legislativo, cuando éste norme una actividad, lo debe hacer sobre los efectos jurídicos perseguidos o deseados y no sobre la manera de cómo se llega a ese fin, lo cual implica que no debería establecer una ley, por ejemplo en materia de Spam, que dijera que los ISP deberán establecer filtros sobre los clientes de correo de tal o cual tecnología.

Este principio encuentra su reconocimiento expreso en nuestro país, en la **LEY 19.799 DE FIRMA ELECTRÓNICA Y SERVICIOS DE CERTIFICACIÓN**[70], la cual en su artículo 1º inciso 2º dispone ***"Las actividades reguladas por esta ley se someterán a los principios de libertad de prestación de servicios, libre competencia, neutralidad tecnológica, compatibilidad internacional y equivalencia del soporte electrónico al soporte de papel."***

En lo que respecta al poder ejecutivo, el Gobierno debe garantizar a través de políticas públicas, que la creación y conservación de los datos y documentos de interés público se realicen de modo tal que no privilegie a ningún tipo de tecnología en particular. No nos referimos en este punto a la imposición de lineamientos obligatorios en lo relativo a las plataformas de hardware o de software, como ocurre principalmente en Europa, por ejemplo, en el debate sobre si las oficinas públicas deberían o no utilizar, obligatoriamente, software de código abierto; sino a la forma en que se crea y conserva la información en sí. No se puede permitir que datos y documentos públicos sean conservados en formatos cerrados o propietarios, sobre todo aquellos de carácter comercial. Es indispensable aplicar estándares internacionales abiertos (por ejemplo, XML) que garanticen un acceso universal a futuro.

En cuanto al poder judicial, este principio se plasma cuando el Juez llega a su decisión basado en los antecedentes de hecho y derecho, más allá de la forma en que estos hayan sido presentados o la tecnología ocupada.

Pero por que hablamos, que este principio es la representación de un

70 Publicada en el Diario Oficial el 12 de abril de 2002

Derecho Fundamental. La razón es simple, este principio no es ni más ni menos que una nueva manifestación de la "**IGUALDAD**", "**SEGURIDAD JURÍDICA**" y "**EL LIBRE EJERCICIO DE UNA ACTIVIDAD ECONÓMICA**".

B.- Equivalencia Funcional.

Este principio se refiere básicamente a que el contenido de un documento electrónico surte los mismos efectos que el contenido de un documento en soporte papel. La equivalencia funcional implica aplicar a los mensajes de datos un principio de no discriminación respecto de las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas.
Se puede decir que aquello que tecnológicamente cumple las mismas funciones de una institución jurídica tradicional, debe ser regulado de la misma manera.

El ejemplo más claro está dado por la llamada Firma electrónica, ya que la misma ley, en la primera parte de su artículo 3º señala ***"Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, públicas o privadas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel."***

Sin duda otro clarísimo ejemplo esta dado por el tratamiento que da el legislador a la correspondencia tradicional, y que debiera reflejar en la correspondencia electrónica.

La equivalencia funcional, no es más que una actualización o consecuencia, de las garantías de la "**IGUALDAD ANTE LA LEY**" y el principio de "**IGUALDAD Y NO DISCRIMINACIÓN**"

C.- La Equivalencia Normativa.

También llamada principio de "**la compatibilidad internacional**", reconocida en el inciso 2º de la ley de Firma electrónica chilena, busca sencillamente que todos los actos que se realicen por la red, no den una sensación de impunidad a las personas que realizan actividades reñidas con la ley o la moral, y que dicho sentimiento no ataque a quienes se puedan ver afectados.

Se busca a través de este principio, que exista una conciencia universal de la protección de las garantías personales.

Por ejemplo, la mayoría de las leyes sobre Protección de Datos, contemplan la existencia de un ente controlador al cual se le entrega la superintendencia de estos registros catastrales, que permite de manera cierta dar la debida protección que se persigue con dichas normas. En Chile, dicho organismo no existe y no fue contemplado por la ley, de manera que el control que permitiría a los ciudadanos obtener la debida protección no existe, haciendo incluso casi impracticable el llamado Habeas Data, lo cual sin duda el día de mañana, en atención a este principio, internacionalmente, podrían cerrar las puertas de sus bases de datos a nuestro país, toda vez que no existen las garantías de un debido tratamiento de los datos en Chile.

Otro ejemplo internacional, son la **Ley Modelo de Firma Electrónica de la Uncitral**[71], o el **Convenio Europeo del Cibercrimen** que busca asegurar la persecución en todos los países parte.

[71] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI)

Obviamente, este es un punto de suma importancia a la hora de legislar sobre el Spam, por lo que será necesario preferentemente atender a los intentos de leyes modelos al respecto, de manera de no establecer una ley que la práctica no cumpla ninguna función real, y que incluso pueda convertirse en un imán para quienes practican el Spam.

D.- Principio de la Mínima Intervención

Este principio en términos simples, implica que la labor del legislador en situaciones como las en estudio, debe dictar leyes modificatorias, que permitan actualizar los antiguos cuerpos normativos a las actuales condiciones tecnológicas.

Por ejemplo, siempre se ha dicho que lo lógico en Chile habría sido dictar una ley que modificara el Código Penal, haciéndolo extensivo a los delitos informáticos y no haber dictado una ley independiente de 4 artículos, como ocurrió con la ley 19.223

La razón que doctrinariamente se da, es no crear nuevos Bienes Jurídicos innecesarios, ya que siempre encontrará su tutela un Bien Jurídico, ya existente.

Este principio, como parte del Derecho Informático, y no sólo como parte del Derecho Penal, debe atender necesariamente a su utilidad y no un elemento que estorbe la realidad. En efecto, como se señala en el artículo denominado **"El Documento Electrónico. Aspectos Procesales"**[72], publicado en la Revista Chilena de Derecho Informático implica ***"que las***

[72] CANELO Figueroa, Carolina, ARRIETA Cortés, Raúl, MOYA García, Rodrigo y ROMO Labish, Rodrigo. El documento electrónico. Aspectos Procesales. Revista Chilena e Derecho Informático. Nº 4. Mayo 2004. Pág. 81 y ss. Universidad de Chile. Facultad de Derecho. Centro de Estudios en Derecho Informático. Santiago. Chile. ISBN: 0717-9162

normas que se dictan en la materia deben ser las estrictamente necesarias para la debida adecuación del sistema jurídico a las condiciones tecnológicas. Por lo tanto, si con el objetivo de dar eficacia y coherencia al sistema jurídico son imprescindibles ciertas modificaciones legislativas, se requiere prudencia al momento de normar, sobre todo en aquellas materias en que la regulación pueda significar una alteración de las categorías jurídicas tradicionales."

Unido a lo anterior, no hay que olvidar jamás, que en los tiempos actuales la evolución de las TICs es tan rápida y prácticamente imperceptible, que muchas leyes cuando sean aprobadas y publicadas, ya se encontraran obsoletas y sin aplicación práctica; por ello es aconsejable atender a la autorregulación, como se ha ido dado en el tiempo con las grandes potencias, y que de una u otra manera ha venido a dar fuerza nuevamente a la llamada costumbre jurídica.

Por ello, a la hora de legislar respecto del Spam, habrá que ver todas las posibilidades existentes, acordes a la realidad nacional, considerando leyes vigentes, idiosincrasia, costumbres, etc.

III.- REGULACION INTERNACIONAL

Para nadie es un misterio, que esta materia que en nuestro país se encuentra en pañales, ya ha sido abordada al menos desde principios del presente siglo, por distintos países y comunidades internacionales. Sin duda, en dichos Estados se han producido avances, y también se han detectado la problemática de legislar y sancionar respecto de esta figura, básicamente por los problemas mencionados y descritos con anterioridad en este trabajo.

No obstante ello, es interesante revisar y poder tomar nota, de acciones que posiblemente ayuden a otros países, posiblemente mas atrasado en el desarrollo tecnológico, pero que por la globalización, mas temprano que tarde se verán afectado por ello, y deberán tomar cartas en el asunto, siendo sus posibilidades de éxito un poco mayor al atender a la experiencia internacional.

Por ello, analizaremos las distintas legislaciones al respecto, especialmente la de la Comunidad Europea, la Norteamérica, algunos esbozos de legislación en Latinoamérica, así como las experiencias africanas, asiáticas y australianas.

A.- La experiencia de la UE

A raíz del creciente aumento de los Correos electrónico no deseados o solicitados, que se produjo en el año 2002, alcanzando el 50% del tráfico de correo electrónico, superando el 7% en el año 2001, en Julio de 2002 se

dictó la **DIRECTIVA 2002/58/CCE[73] SOBRE LA INTIMIDAD Y LAS COMUNICACIONES ELECTRÓNICAS**, introduciendo para la Unión Europea el principio del "***consentimiento previo***" a través de lo que denominan el "registro de inclusión" aplicable tanto para el envío de correos electrónicos con fines comerciales, como para los mensajes SMS o MMS enviados a través de teléfonos móviles. Dicha Directiva establecía varias medidas que los Estados miembros debían aplicar para las comunicaciones comerciales a más tardar el 31 de octubre de 2003[74].

Esta medida tomada desde la trinchera de la legislación, a criterio de sus autores, obviamente no permite acabar con el SPAM, pero era el inicio de una guerra que debía contar con mas aliados, especialmente de ***"los Estados miembros y sus autoridades públicas, en las soluciones técnicas y la autorregulación por parte de la industria y en la sensibilización de los consumidores"[75].***

Dicha directiva en definitiva fue formulada como un hito para alcanzar el consenso para frenar la proliferación del spam si todos los interesados, Estados miembros, autoridades públicas, proveedores de servicio Internet y correos, consumidores y usuarios de Internet, ejercen su papel, tomando las acciones que les competen a cada uno.

Lo que es importante señalar, que pese a que la CEE manifiesta fines altruistas al leer y estudiar sus distintas normas en la materia, más allá de

---

73 Publicado en Diario Oficial de las Comunidades Europeas. 31 de julio de 2002. Actualización permanente. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:ES:PDF

74 Directiva 2002/58/CCE. Artículo 13. Sobre la intimidad y las comunicaciones electrónicas. Diario Oficial de las Comunidades Europeas. [en línea] Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:ES:PDF

75 Comunicación de la Comisión al parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones comerciales no solicitadas o spam. Celebrado en Bruselas, el 22 de enero de 2004. [en línea] Disponible para consulta y descarga en:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:318:0024:0026:ES:PDF

estar protegiendo efectivamente la intimidad de las personas, esta mas preocupada de que no se dañen sus economías, ya que mas allá que los usuarios limiten o dejen de usar estos medios de comunicación (eficientes al ser bien usados) ya que como se señala en el documento citado, ***"Internet y otros medios de comunicaciones electrónicas (p. ej., el acceso de banda ancha, el acceso inalámbrico o las comunicaciones móviles) deben constituir un elemento esencial del crecimiento de la productividad en una economía moderna"[76].***

La ya mencionada Directiva 2002/58/CEE sobre la intimidad y las comunicaciones electrónicas exigía que los Estados miembros prohibieran el envío de mensajes comerciales no solicitados por correo electrónico u otro servicio de mensajería electrónica como el SMS o el MMS, a menos que se hubiera obtenido previamente el consentimiento del abonado a estos servicios. Esto es lo que se llama ***"principio del consentimiento previo"*** y que en Europa era sólo era aplicable a las comunicaciones vía Fax y las llamadas telefónicas vía servicios de audiotexto.

A fin de lograr cumplir lo anterior se dispuso que:

a) ***El envío de mensajes electrónicos con fines comerciales queda sometido expresamente al "consentimiento previo" de los abonados[77]; eso si que con una excepción respecto de mensajes de correo electrónico o mensajes cortos a través de teléfonos móviles, cuando sean enviados por una empresa a clientes existentes y***

76 Comunicación de la Comisión al parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre las comunicaciones comerciales no solicitadas o spam. Celebrado en Bruselas, el 22 de enero de 2004. [en línea] Disponible para consulta y descarga en:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:318:0024:0026:ES:PDF

77 Directiva 2002/58/CEE E . Artículo 13. Comunicaciones no solicitadas. Apartado 1. Sólo se podrá autorizar la utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa respecto de aquellos abonados que hayan dado su consentimiento previo.

referidos a servicios o productos similares, pero que sean personas naturales, y quedando su aplicación a las personas jurídicas a criterio de cada Estado miembro[78]. Esto es lo que en doctrina se llama "autorización por venta" o "autorización previa suave", pero para no dañar el principio general, las empresas deben indicar expresamente, desde el momento en que obtiene los datos, que éstos podrían ser utilizados por ellos, con fines de venta directa y, si procediere, que pueden transmitirse a terceros a tal efecto y ofrecer al consumidor la posibilidad de oponerse gratuitamente y de forma simple; además de la posibilidad de solicitar posteriormente de igual manera la exclusión de las listas de correos[79].

b) ***Se declaro la ilicitud expresa de la acción de enviar un a comunicación disimulando u ocultando la identidad del remitente o emisor[80].***

c) ***Todos los mensajes electrónicos enviados deben contener una dirección de respuesta válida donde el abonado pueda pedir que no se le envíen más mensajes.***

Es importante señalar, que las disposiciones de la Directiva 95/46/CE sobre protección de datos relativas a recursos judiciales, responsabilidad y sanciones son aplicables a las disposiciones de la Directiva sobre

---

79 Directiva 2002/58/CEE E . Artículo 13. Comunicaciones no solicitadas. Apartado 2. No obstante lo dispuesto en el apartado 1, cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior.

80 Directiva 2002/58/CEE E . Artículo 13. Comunicaciones no solicitadas. Apartado 4. Se prohibirá, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación, o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones.

intimidad y comunicaciones electrónicas, incluidas las relativas a comunicaciones no solicitadas. En efecto el artículo 15 dispone que:

"Artículo 15. Aplicación de determinadas disposiciones de la Directiva 95/46/CE

1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea.

2. Las disposiciones del capítulo III sobre recursos judiciales, responsabilidad y sanciones de la Directiva 95/46/CE se aplicarán a las disposiciones nacionales adoptadas con arreglo a la presente Directiva y a los derechos individuales derivados de la misma.

3.El Grupo de protección de las personas en lo que respecta al tratamiento de datos personales, creado por el artículo 29 de la Directiva 95/46/CE, ejercerá también las funciones especificadas en el artículo 30 de dicha Directiva por lo que se refiere a los asuntos

objeto de la presente Directiva, a saber, la protección de los derechos y las libertades fundamentales y de los intereses legítimos en el sector de las comunicaciones electrónicas."

Lo que se buscaba con esta remisión expresa a la norma general, era obviamente que los Estados miembros velaran para que en caso de infracción, existieran recurso y sanciones, ya que es la manera adecuada para que cualquier garantía o derecho garantizado tenga su real protección y eventual reparación; pues es un criterio general de la Comisión que ellos no pueden tomar dichas providencias respecto de los nacionales de los Estados miembros.

Además de las regulaciones ya mencionadas, y relacionadas directa o indirectamente con el Spam, la CEE y los Estados miembros también se han referido a otras materias. En efecto, la CEE se refirió a la práctica de la ***"recolección de direcciones de correo electrónico",*** es decir, la recogida automática de datos personales en Internet (Web en general, chats, etc), al declararla ilícita en virtud de la Directiva 95/46/CE sobre protección de datos, esté o no efectuada de manera automática con ayuda de un programa informático.

Además hay que señalar que respecto del spam fraudulento, es ilícito en virtud de las normas existentes en la UE sobre publicidad engañosa y prácticas comerciales desleales[81].

También es dable citar las normas de la **DIRECTIVA 2000/31/CE RELATIVA A DETERMINADOS ASPECTOS JURÍDICOS DE LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN, EN PARTICULAR**

81 Directiva 84/450/CEE del Consejo, de 10 de septiembre de 1984, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de publicidad engañosa Disponible para consulta y descarga en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31984L0450:ES:HTML

EL COMERCIO ELECTRÓNICO EN EL MERCADO INTERIOR en el sentido de que las "comunicaciones comerciales" deben ser claramente identificables)[82].

Por último a nivel de Estados miembros, se encuentran las regulaciones respecto de los correos electrónicos con contenidos pornográficos o discriminatorios, que si bien pueden ser de contendido nocivos, no son en estricto derecho ilícitos, y ha sido la legislación de los distintos países la que ha sancionado duramente en algunos casos estas acciones.

Vencido el plazo del 31 de octubre de 2003 que la Comisión había dado a los Estados miembros para aplicar las medidas acordadas por la Directiva 2002/58, y atendido el hecho de que varios de ellos no lo cumplieron, en noviembre de 2003, la Comisión inicio algunos procedimientos sancionatorios en contra de los estados infractores.

Con el fin de mejorar y lograr la real aplicación de la Directiva señalada, la **COMISION DE COMUNIDADES EUROPEAS** se reunió en Bruselas el 22 de enero de 2004, naciendo una serie de propuestas de acciones a seguir por los estados miembros, sus autoridades, empresas y consumidores, todas ellas tendientes a obtener la aplicación y cumplimiento de las normas y regulaciones; generar autorregulaciones y acciones técnicas, así como acciones de sensibilización, que analizaremos ordenadamente.

---

82 Directiva del Parlamento Europeo y del Consejo de 8 de junio de 2000, DO L 178 de 17.7.2000.
Por regla general, las «comunicaciones comerciales» deben respetar las disposiciones nacionales aplicables en el Estado miembro en que esté establecido el prestador de servicios. Esta norma no se aplica, sin embargo, a la licitud de las comunicaciones no solicitadas por correo electrónico (véase el artículo 3 de la Directiva sobre comercio electrónico y su anexo). En los casos (limitados) en que la Directiva 2002/58/CEE E no proteja a las personas físicas contra las comunicaciones comerciales no solicitadas (p. ej. personas físicas que no sean abonados), los Estados miembros deberán garantizar, con arreglo a la Directiva sobre comercio electrónico, que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente los registros de exclusión en los que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y los respeten (véase el artículo 7 de la Directiva sobre comercio electrónico).

Como se puede observar este no ha sido un proceso fácil ni exento de dificultades en los acuerdos, los modos de operar y además, los que generan la extraterritorialidad de la normativa a aplicar. Asimismo, no basta con los acuerdos adoptados como comunidad, requiere además la elaboración de estrategias y acciones nacionales

La CEE y las autoridades involucradas se propusieron, entre otros principios, los siguientes:

- ***Establecer los conductos eficaces a las víctimas para ejercer sus acciones en defensa de sus derechos personales y patrimoniales, sea buscando sanción o persiguiendo que se indemnicen los perjuicios que le hubieran ocasionado a través de estas irrupciones a su privacidad. Esto implica que el afectado debe contar con mecanismos simples y directos para poner en conocimiento de la autoridad la infracción reclamada y el daño causado.***
- ***Crear los organismos pertinentes, o cuando sean necesario dotar los ya existentes de la competencia y facultades necesarias de investigación y sanción.***
- ***Crear mecanismos fluidos de comunicaciones entre los países miembros, de manera tal que puedan actuar en forma coordinada, facilitando la acción de los órganos investigadores y sancionadores, aún más allá del país en que tengan su asiento.***
- ***Crear las bases necesarias de cooperación con terceros países, a fin de extender la aplicación de las soluciones adoptadas por la CEE o elaborar otras, y***
- ***Generar las instancias de cooperación con el sector privado a***

fin de detectar, entre otros datos relevantes en la investigación, los remitentes de spam.

Las razones que llevaron a intervenir, básicamente atendía a una serie de problemas que no podían ser ignorados, entre los cuales se destacan los siguientes:

a.- Diversidad de autoridades que están a cargo de la regulación en los distintos países.

Cada país tiene una autoridad a cargo de este problema, en algunos es la autoridad que asume la protección de datos (APD), en otros, la que asume la reglamentación en los temas de comunicaciones (ANR), la que asume la protección de los consumidores (APC), o la que tiene la facultad de ejecutar las sanciones aplicables. Y además, es necesario considerar que a menudo el envío de spam está asociado a infracción de normas de protección de datos, como por ejemplo, la recopilación de direcciones de correo electrónico, y otras tantas veces, asociadas a actividades ilícitas como la irrupción en forma ilegal a PC o a servidores. Las autoridades en cada país a cargo de la generación y aplicación de la normativa no son siempre las mismas en cada país y a esto es necesario sumarle la cantidad de países miembros con sus propias autoridades, lo que constituye un problema casi insalvable de coordinación y generación de normas únicas.

b.- Diversidad en la forma de iniciar un proceso.

En la mayoría de los países, una denuncia genera una investigación. Muchas veces se producen contactos previos del consumidor afectado a la empresa, como una etapa previa a la denuncia. En algunos países se ha establecido la denuncia como el marco de la autorregulación, y en otras

ocasiones la autoridad incluso puede actuar de oficio. Todo lo anterior no excluye las acciones que se pueden ejercer ante la autoridad judicial.

En algunos países, las autoridades a cargo de la protección de datos no pueden accionar directamente contra personas jurídicas, ni tampoco se tiene la facultad coercitiva de hacer cumplir las normas mediante sanciones, lo que hace necesario tener que iniciar acciones ante la autoridad judicial para estos efectos.

Se ha considerado como un método eficaz para aplicar el régimen de consentimiento previo lo constituiría llegar a un ansiado equilibro entre la legislación, la imposición de las normas y la autorregulación, respecto de lo cual los países miembros fueron llamados a evaluar.

Asimismo, se solicitó la elaboración de estrategias nacionales tendientes a lograr la cooperación y coordinación entre las autoridades responsables, dentro del país, encargadas de la protección de datos, derechos del consumidor y de las comunicaciones, evitando de este modo los conflictos de competencia entre dichas autoridades y la duplicidad de funciones.

Con el objeto de facilitar el intercambio de información y a la larga fomentar un trabajo coordinado, se creo un Grupo informal en línea sobre las comunicaciones comerciales no solicitadas. Dicho grupo, con el apoyo de los países miembros tendría como función, facilitar y coordinar los trabajos que desarrollarán en las acciones descritas precedentemente y tendría además como importante labor, la de sensibilizar y aportar soluciones técnicas. Este Grupo estaría integrado por representantes de las administraciones nacionales competentes así como los servicios de la Comisión, eventualmente podrá incorporar otros estamentos a fin de garantizar la participación de todas las partes interesadas.

Se dispuso que el trabajo realizado por este Grupo fuera sometido al Comité de Comunicaciones (COCOM) y/o al Grupo de Trabajo de Protección de los Datos, y finalmente elaborar los criterios de evaluación comparativa de las diferentes medidas que se propongan.

La Comisión estableció que era condición previa, que los Estados miembros y las autoridades competentes evalúen la eficacia de sus mecanismos para hacer cumplir la normativa (recursos y sanciones, mecanismos de denuncia, cooperación interna en la UE y cooperación con terceros países y seguimiento), asimismo los Estados miembros deben también elaborar estrategias nacionales con el fin de garantizar la cooperación entre las APD, las APC y las ANR, y evitar el conflicto de competencias y la duplicación de esfuerzos entre las distintas autoridades.
A continuación se enumerarán en forma resumida las acciones descritas y acordadas, para todos los ámbitos involucrados:

I. Acciones dependientes de la Comisión o de los servicios de la Comisión.

Estas acciones guardan diversas relaciones entre sí y deberían aplicarse, en la medida de lo posible, en paralelo y de manera integrada.

a.- Recursos y sanciones eficaces

Al respecto se señalo que era necesario:

a.1.- Evaluar la eficacia de los recursos que se conceden a las víctimas o afectados, a fin que el procedimiento que se establezca sea rápido, asequible y eficaz para obtener la protección, la sanción y la indemnización por los daños y perjuicios causados. En los Estados miembros que no

disponen de vías de recurso administrativo, deben prever la creación de tales vías a fin de hacer aplicar las nuevas normas;

a.2.- Dotar a las autoridades competentes de las facultades de investigación y ejecución necesarias.

a.3.- Las sanciones deben revestir las características tales y las autoridades la facultades necesarias para logra su aplicación efectiva, incluso más allá de las fronteras del país en se comete la infracción.

b.- Mecanismos de denuncia

En lo que a este item, se adoptó el acuerdo de:

b.1.- Establecer mecanismos de denuncia adecuados, tales como los buzones electrónicos que recojan las denuncias de los usuarios, con la debida información para éstos;

b.2.- Difusión de la experiencia con el uso de los buzones electrónicos entre los países miembros.

c.- Denuncias transfronterizas y cooperación en materia de cumplimiento dentro de la UE

Para darle eficacia a las denuncias y sanciones, se determino en calidad de esencial:

c.1.- La colaboración y comunicación entre los países miembros, de modo tal que las fronteras no sean un obstáculo adicional para la sanción de las prácticas del spam.

C.2.- Se propuso un Reglamento relativo a la cooperación entre autoridades nacionales encargadas de la aplicación de la legislación en materia de protección de los consumidores para abordar problemas fronterizos; invitando a los países miembros a (a) evaluar los procedimientos actuales respecto al tratamiento de las denuncias fronterizas; (b) intensificar las acciones de coordinación e intercambio de información entre las autoridades encargadas para cumplir las nuevas disposiciones y de éstas con las responsables de las formas particulares de spam, como por ejemplo el spam fraudulento o "scam", el spam pornográfico, etc.; (c) aprobar el Reglamento mencionado y evaluar el extenderlo sobre temas de protección de intimidad y comunicaciones electrónicas; (d) Suprimir los obstáculos existentes al intercambio de información y a la cooperación, pudiendo ser útil disponer de un mecanismo de enlace y red de apoyo que pudiera basarse en programas de la Comisión ya existentes., como IDA[83].

c.3.- Establecer la cooperación con terceros países

Con dicho fin se determinó que era esencial (a) Participar activamente en los foros multilaterales (por ejemplo la OCDE) con el fin de elaborar soluciones a nivel internacional; (b) reforzar o iniciar, la cooperación bilateral con los terceros países; (c) estudiar, con la Comisión, qué iniciativa específica podría adoptar ésta para facilitar la cooperación

83 IDA o IDABC (Interoperable Delivery of European e-Government Services to public Administrations, Businesses and Citizens). Este organismo utiliza las posibilidades ofrecidas por las tecnologías de información y de comunicación para apoyar la entrega de los servicios fronterizos del sector público a los ciudadanos y a las empresas en Europa, para mejorar la eficacia y la colaboración entre las administraciones públicas europeas y contribuya a hacer Europa un lugar atractivo para vivir, para trabajar y para invertir. Para alcanzar sus objetivos, las recomendaciones de las ediciones de IDABC, desarrollan soluciones y proporcionan los servicios que permiten a las administraciones nacionales y europeas comunicarse electrónicamente y ofrecer servicios públicos modernos a los negocios y a ciudadanos en Europa. El programa también proporciona financiamiento a los proyectos destinados a los requisitos de la política europea para así mejorar la cooperación entre las administraciones a través de Europa.
http://ec.europa.eu/idabc/en/chapter/3

internacional; (d) cooperar con el sector privado, en particular ISPs y ESPs, con el fin de detectar los remitentes de spam, a reserva de las garantías jurídicas apropiadas; y (e) asegurarse de disponer de la información y las estadísticas requeridas para hacer cumplir la normativa, en cooperación con la industria cuando proceda, y teniendo en cuenta los trabajos sobre medición que lleva a cabo actualmente la OCDE.

II) Acciones técnicas y de autorregulación por parte del sector

Estas medidas se refieren especialmente a los agentes de mercado, en ámbitos tales como las disposiciones contractuales, códigos de conductas, las prácticas de comercialización aceptables, los mecanismos alternativos de solución de conflictos y soluciones técnicas como el filtrado y la seguridad de los servidores.

Se consideran para estos efectos a los actores del mercado, tales como ISPs, ESPs, operadores de redes móviles, empresas de software, empresas de venta directa; los cuales deben convertir el régimen de consentimiento previo en una práctica cotidiana, en cooperación con las asociaciones de consumidores y usuarios y las autoridades competentes cuando proceda, y en particular:

a.- Acciones de autorregulación

Entre estas deben:

a.1.- Evaluar, y si es preciso adaptar, las prácticas contractuales de los proveedores de servicios (ISP, ESP, operadores móviles) en relación con sus abonados y sus socios comerciales a las nuevas disposiciones; facilitar información sobre el filtrado y suministrar quizás opcionalmente a los clientes programas o servicios de filtrado; - adaptar las prácticas de venta

directa al régimen de consentimiento previo y ponerse eventualmente de acuerdo sobre métodos concretos de recogida de datos personales conformes al Derecho (p. ej., sistemas de consentimiento "doble" o "confirmado");

a.2.- Elaborar y difundir códigos de buenas prácticas eficaces, como ha ocurrido con la iniciativa **FEDMA**[84]; conformes al régimen de consentimiento previo, en cooperación con el Grupo de trabajo sobre protección de datos del artículo 29 o con las autoridades nacionales competentes cuando proceda; - estudiar la posible utilización de etiquetas para los mensajes electrónicos que respetan el régimen de consentimiento previo y de bases de datos para ayudar a los usuarios (y a los filtros) a reconocerlos, de conformidad con la Directiva sobre comercio electrónico;

a.3.- Utilizar, o crear si es necesario, mecanismos de denuncia y mecanismos alternativos y extrajudiciales de solución de litigios en el marco de la autorregulación, que sean eficaces y se basen en iniciativas existentes en la medida de lo posible, tal como ocurrió con la **EEJ-NET**[85]. Para ser eficaces, estos mecanismos deben cumplir con ciertas condiciones relativas a su organización y promoción, así como a las medidas previstas para garantizar la ejecución de los resuelto.

84 Federation of European direct and interactive marketing (Federación Europea de Mercadeo directo e interactivo) , creada en 1997, y reúne a 298 federaciones nacionales de asociaciones de marketing directo

85 EEJ-NET (European Extra-Judicial Network) o RED EJE. Esta red tenía por objetivo establecer una red de órganos nacionales de solución extrajudicial de los litigios para permitir una solución rápida y eficaz de los litigios de consumo transfronterizos mediante la utilización de los nuevos medios de comunicación, en especial Internet. Fue creada el 16 de octubre de 2001 por el Comisario David Byrne y la presidencia belga como proyecto piloto de un año, pero en atención a su éxito, la Comisión Europea pidió al Consejo de Ministros que la prorrogara por un año. El Consejo aprobó la propuesta y amplió la fase piloto hasta el 31 de diciembre de 2003. Esta red intentaba ayudar a los consumidores a resolver los litigios transfronterizos que los enfrentaban a las empresas que suministran bienes o servicios defectuosos, dirigiéndolos hacia los organismos de resolución alternativa de litigios. http://europa.eu/scadplus/leg/es/lvb/l32043.htm

b.- Acciones técnicas

Al respecto se estableció que:

b.1.- Velar para que los diferentes sistemas de filtrado sean compatibles con el régimen de consentimiento previo y demás exigencias del Derecho de la UE, incluidas los vinculadas a la confidencialidad de las comunicaciones.

b.2.- Los Estados miembros y a las autoridades competentes deben clarificar las condiciones jurídicas para el funcionamiento de los distintos tipos de programas de filtrado en el país en cuestión, y en particular los requisitos relacionados con el respeto de la intimidad.

b.3.- Los proveedores de servicio deben considerar las consecuencias para los usuarios de los «falsos positivos», los «falsos negativos» y determinadas formas de filtrado basado en los contenidos, así como de los posibles problemas de responsabilidad asociados. Los usuarios deben tener la posibilidad de decidir qué se hace con el spam entrante, en función de sus necesidades.

b.4.- Cooperar estos mismos con las partes interesadas para desarrollar técnicas de reconocimiento de los mensajes comerciales legítimos, es decir, que corresponden a las prácticas comerciales aceptadas en virtud del Derecho comunitario, utilizando por ejemplo etiquetas.

b.5.- Ofrecer una opción de productos o servicios de filtrado a los clientes que lo soliciten, e informarlos sobre los propuestos por terceros.

b.6.- Garantizar la seguridad de sus servidores, de manera que no funcionen en el modo abierto, salvo que esté justificado. Lo mismo cabe

decir de los Proxy abiertos.

III.- Acciones de sensibilización por parte de los Estados miembros, el sector y las asociaciones de consumidores o usuarios

Se ha invitado a los Estados miembros y las autoridades competentes a programar campañas que tengan como objetivo sensibilizar a los actores de este proceso respecto de las acciones que se deben desarrollar o a apoyar dichas campañas. Todas las partes implicadas, desde los Estados miembros y las autoridades competentes hasta las asociaciones de consumidores y usuarios, pasando por las empresas, deberían participar en las campañas de información práctica en materia de prevención, prácticas de comercialización aceptables y soluciones y acciones técnicas y jurídicas a disposición de los usuarios, y en particular:

a.- Orientar las acciones hacia las empresas implicadas en la venta directa o que la utilizan, los consumidores abonados a servicios de correo electrónico, incluidos los servicios SMS, y finalmente, a los proveedores de servicios de correo electrónico, incluidos los proveedores de servicios móviles.

b.- Facilitar a las empresas y/o a los consumidores:

b.1.- la información básica pero global, sobre las nuevas normas y sus derechos en virtud de ellas;

b.2.- la información práctica sobre las prácticas de comercialización aceptables en el marco del régimen de consentimiento previo, clarificando, en particular, el concepto de recogida legítima de datos personales;

b.3.- la información práctica para que los consumidores sepan cómo evitar el spam (por ej. utilización de los datos personales, etc.);

b.4.- la información práctica para los consumidores sobre productos y servicios disponibles para evitar el spam (p. ej., filtrado, seguridad);

b.5.- la información sobre las medidas prácticas que deben adoptarse en caso de recibir spam, incluidos los mecanismos de denuncia;

Todo lo anterior debe estar relacionado con los códigos de conducta del sector eficaces, a los mecanismos de denuncia, a las etiquetas, tales como las marcas de confianza; y a los sistemas de certificación eventualmente disponibles.

La participación de las asociaciones sectoriales y de consumidores adquiere gran importancia en este contexto. Conviene garantizar la coordinación de las distintas iniciativas posibles.

.

IV – Acciones que deben aplicar la Comisión o sus servicios

La Comisión efectuará un seguimiento de la aplicación de las acciones resumidas en 2004, en particular a través del Grupo informal sobre comunicaciones no solicitadas, y evaluaría, a más tardar para finales de 2004, si hacen falta medidas suplementarias o correctivas.

En términos generales, señala que la Comisión seguirá supervisando atentamente la aplicación de la Directiva y es su objetivo procurar, en particular, que las medidas de transposición nacionales prevén sanciones reales, incluidas las de tipo económico o penal, en caso de violación de las exigencias correspondientes (la Comisión inició en noviembre de 2003 procedimientos de infracción contra varios Estados miembros por ausencia

de notificación de sus medidas de transposición nacionales). Los servicios de la Comisión están dispuestos a ayudar a los Estados miembros si resulta necesario, apoyando las gestiones y desarrollo de las acciones en cada uno de ellos.

Los servicios de la Comisión pedirán al Grupo de trabajo sobre protección de datos del artículo 29 que apruebe cuanto antes un dictamen sobre algunos conceptos utilizados en la Directiva de la intimidad y las comunicaciones electrónicas, con el fin de contribuir a una aplicación uniforme de las medidas nacionales adoptadas en virtud de la Directiva.

Los servicios de la Comisión han comenzado a estudiar, con los Estados miembros y las autoridades nacionales encargadas de la imposición, los mejores medios de garantizar la aplicación transfronteriza en el territorio de la UE, así como con los terceros países.

La Comisión procurará determinar los mejores medios de dar continuidad a los resultados de la Cumbre Mundial sobre la Sociedad de la Información de 2003 en la UE.

La Comisión ha publicado una convocatoria de propuestas en el marco del programa sobre la seguridad de Internet que permite proponer proyectos de lucha contra el spam en varias acciones; la Comisión prepara actualmente una propuesta de programa continuador que propondrá financiar nuevas medidas, en particular para luchar contra el spam.

Finalmente respecto de esta comunicación de 2003, se estableció que los servicios de la Comisión seguirán facilitando información sobre las bases del régimen de consentimiento previo en el sitio web EUROPA, transmitirán también, mediante hiperenlaces, a los aspectos nacionales de

la aplicación así como a las cifras y tendencias básicas en materia de spam cuando se disponga de ellas, recurriendo además, a los centros europeos de información empresarial para difundir información sobre las nuevas normas.

Por otra parte en Noviembre de 2006, se dictó una nueva comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al comité de las regiones, sobre la lucha contra el SPAM, los programas espía y los programas maliciosos (COM/2006/0688 final)[86].

La razón tomada en consideración por este organismo para dictar la señalada comunicación, estaba dada por el hecho que en su opinión la sociedad en general, ha adquirido la conciencia de lo esenciales que resultan las modernas redes y servicios de comunicaciones electrónicas para la vida cotidiana, tanto en la empresa como en el hogar, y a fin de que los servicios alcanzaran una amplia difusión necesariamente debían apoyarse en tecnologías fiables, seguras y dignas de confianza.

Esta comunicación constituyó la formulación de una estrategia para una sociedad de la información segura, cuyo objetivo es mejorar la seguridad de las redes y de la información en general, invitando y haciendo participes, al sector privado a combatir los puntos vulnerables de las redes y los sistemas de información susceptibles de ser explotados para distribuir spam y programas maliciosos; proponiendo la revisión del marco regulador de la UE, y sugiriendo nuevas normas encaminadas a reforzar la seguridad y la privacidad en el sector de las comunicaciones electrónicas.

Esta comunicación pasa a considerar la evolución del spam, en conjunto

86 Celebrado en Bruselas, 15 de noviembre de 2006. Disponible para consulta y descarga en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:ES:PDF

de otras amenazas tales como los programas espía y los programas maliciosos, normalmente muy unidos entre si y necesarios para su subsistencia.

Se señala en el referido documento que el spam ha experimentado un crecimiento significativo entre el año 2001 y el 2006, pues el índice de 7% de Spam a pasado a representar entre el 50 y el 80 % de los mensajes dirigidos a los usuarios finales.

Aun cuando están contestes que de dicha cifra sólo el 25% pertenece a correos cuyo origen sea la UE, los perjuicios no han sido menores, considerando que a dicha fecha (Noviembre 2006) el costo del spam ascendió a 39.000 millones de euros en el mundo y, para las principales economías europeas, a aproximadamente 3.500 millones en Alemania, 1.900 millones en el Reino Unido y 1.400 millones en Francia.

Agregan que el principal problema radica en el hecho de que el spam se ha convertido en un gran negocio por si mismo; ya que los emisores arriendan o venden a las empresas listas con las direcciones de correo electrónico que han obtenido para fines comerciales; siendo sumamente lucrativo, en atención a la penetración y escasos costos de Internet.

Las razones por la cual el Comité ha pasado a considerar el problema del Spam, junto a los virus y spywares es simple, ya que el correo electrónico no solicitado, de ser una simple molestia en sus inicios ha tomado caracteres de medio de ejecución de delitos, como ocurre con el phishing, el cual induce a los usuarios finales a entregar datos de carácter sensible a través de páginas web que imitan las de empresas auténticas, generalmente bancos, donde el usuario mantiene una cuenta corriente. También han aumentado el envío por correo electrónico o incluyéndolo en

otro software, de programas espías que vigilan y comunican el comportamiento en línea de un usuario, o sencillamente recogen toda la información personal del usuario, tales como contraseñas o los números de sus tarjetas de crédito.

Por su parte, agregan que la difusión de programas maliciosos como gusanos y virus facilita enormemente el envío masivo de mensajes electrónicos no solicitados; pues una vez instalados, permiten al atacante hacerse con el control de un sistema informático infectado y convertirlo en un BOTNET[87], ocultando así la identidad del verdadero emisor del spam, y sin que el propietario del computador sepa que esta enviando spams.

Por ello luego de un análisis de las medidas adoptadas con anterioridad, sugiere una serie de nuevas medidas, cuya eficacia será analizada a fines del año 2008.

Estas medidas al igual que con ocasión del acta de 2003, ya tratada largamente están dirigidas hacia los distintos actores del mercado y sociedad.

V.- Recomendaciones para Los Estados Miembros

Para los Estados Miembros se dan una serie de recomendaciones básicamente en relación con la represión y la cooperación, llamándolos a dar mas prioridad al problema, de manera de tomar medidas contra quienes envían spam, realizan phishing o distribuyen programas espía o maliciosos de forma "profesional"

87 Red o grupo de computadores zombies, controlados por el propietario de los bots. El propietario de las redes de bots da instrucciones a los zombies. Estas órdenes pueden incluir la propia actualización del bot, la descarga de una nueva amenaza, el mostrar publicidad al usuario o el lanzar ataques de denegación de servicio, entre otras. http://antivirus.interbusca.com/glosario/BOTNET.html
Los expertos del sector calculan que los botnets transmiten más del 50 % de los mensajes electrónicos abusivos.

Para ello en primer lugar se requiere obtener una Coordinación e integración a nivel nacional de cada Estado Miembro. Se señala que estos, en virtud de la Directiva sobre la intimidad y las comunicaciones electrónicas y a la Directiva general sobre protección de datos[88], las autoridades nacionales son competentes para actuar contra prácticas ilícitas tales como:

- envió de comunicaciones no solicitadas[89];
- acceso ilícito a equipos terminales, sea para almacenar información, tales como programas publicitarios o adware y programas espías; sea para acceder a la información almacenada en esos equipos[90];
- infectar equipos terminales mediante la inserción de programas maliciosos, tales como gusanos y virus, y convertir un PC en un botnet o usarlo para otros fines[91];
- engañar al usuario para que facilite información sensible, tal como contraseñas o números de tarjetas de crédito, mediante los llamados mensajes de phishing[92].

Agrega el comunicado, recordando que muchas de estas practicas son punibles al amparo del Derecho penal, y citan en particular la Decisión marco relativa a los ataques contra los sistemas de información[93]; en virtud de la cual los Estados miembros deben prever una pena de tres años de prisión como mínimo en su grado máximo, o cinco años cuando se cometan en el marco de una organización delictiva.

---

88 Directiva 95/46/CEE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible para consulta y descarga en: http://derecho.eui.upm.es/DPDPF.pdf
89 Artículo 13 Directiva 2002/58/CCE. Sobre la intimidad y las comunicaciones electrónicas.
90 Artículo 5, apartado 3, Directiva 2002/58/CCE. Sobre la intimidad y las comunicaciones electrónicas.
91 Artículo 5, apartado 3, Directiva 2002/58/CCE. Sobre la intimidad y las comunicaciones electrónicas.
92 Artículo 6, letra a) Directiva 95/46/CEE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
93 Decisión marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques de los que son objeto los sistemas de información. Disponible para consulta y descarga en: http://www.belt.es/legislacion/vigente/Seg_inf/Protecci%C3%B3n%20de%20datos/pdf/decision_16-marzo_05.pdf

Señala la comisión que es de suma importancia que a nivel nacional, los organismos administrativos y/o a las autoridades penales hagan cumplir estas normas, aun cuando lleve aparejado el hecho que para delimitar las competencias se deban tomar y adoptar modificaciones normativas y legislativas del mas alto nivel. Es precisamente este elemento el que la Comisión no ha observado en los distintos Estados Miembros, ya que no se han dictado protocolos de cooperación para el intercambio de información, de datos de contacto, la asistencia y la transferencia de expedientes.

En segundo lugar, agrega que para lograr obtener pruebas fidedignas y confiables, y para poder realizar las investigaciones necesarias y establecer los mejores procedimientos, se requiere que las autoridades obtengan recursos técnicos y jurídicos, de manera de familiarizarse con la forma de trabajar de los delincuentes si quieren combatir con éxito sus prácticas, y mas aun que de una u otra manera, en la medida de lo posible puedan ir un paso mas adelante, y no siempre actuando como reacción.

Al respecto la Comisión señala que "Los mecanismos de presentación de denuncias en línea, con sistemas asociados que permitan registrar y analizar las prácticas maliciosas denunciadas, pueden constituir una herramienta importante. La experiencia ha demostrado que con unas inversiones moderadas pueden obtenerse resultados significativos. La reducción del spam neerlandés se consiguió creando un grupo de cinco empleados a tiempo completo en la OPTA, autoridad neerlandesa, y dotándolo de equipos valorados en 570.000 euros. Apoyándose en esta inversión, la experiencia obtenida en la lucha contra el spam está siendo ahora utilizada para combatir otro tipo de problemas"[94].

94 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al comité de las regiones, sobre la lucha contra el SPAM, los programas espía y los programas maliciosos.

En tercer lugar hacen presente el alcance transfronterizo del Spam, por lo cual las autoridades de un país dependerán a menudo de las autoridades de otros para perseguir a los emisores del spam y, a la inversa, podrán recibir solicitudes de realización de investigaciones procedentes de otros países; y aun cuando pueda parecer que no vale la pena el dedicar recursos en perseguir ilícitos cometidos en otro país, el resultado es optimo, pues implica una eventual protección anticipada.

En virtud de lo anterior, la Comisión insta a los Estados miembros y a las autoridades competentes a[95] que:

- establezcan líneas de responsabilidad claras para los organismos nacionales participantes en la lucha contra el spam;
- garanticen una coordinación efectiva entre las autoridades competentes;
- consigan la participación de los agentes del mercado a nivel nacional, apoyándose en sus conocimientos técnicos y en la información disponible;
- garanticen que las actividades encaminadas a hacer cumplir la legislación dispongan de los recursos adecuados;
- se adhieran a los procedimientos del cooperación internacional y den curso a las solicitudes de asistencia transfronteriza.

VI.- Medidas para la Industria

Respecto de las medidas que podría adoptar el sector de la industria

---

Bruselas, 15 de noviembre de 2006. Disponible para consulta y descarga en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:ES:PDF

95 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al comité de las regiones, sobre la lucha contra el SPAM, los programas espía y los programas maliciosos. Bruselas, 15 de noviembre de 2006. Disponible para consulta y descarga en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0688:FIN:ES:PDF

apuntan hacia dos ámbitos, uno fomentar la confianza de los consumidores y dos, frenar el envío de mensajes electrónicos abusivos, básicamente por el eventual contendido de programas espías.

En primer lugar se insta a dar la mayor Información al consumidor, y hacerles presentes que muchas ofertas de software pueden incluir la instalación de programas adicionales, que pueden actúar como espías vigilando el comportamiento de los usuarios finales, están realizando un tratamiento de datos personales, actividad ilegal si no cuenta con el consentimiento informado del usuario. En muchos casos no se obtiene dicho consentimiento, o se obtiene escondiéndolo en la letra pequeña de un prolijo acuerdo de concesión de licencia el usuario final. Por ello, se llama a las empresas que ofrecen productos de software a exponer de forma clara y visible todas las condiciones de la oferta, y en particular si incorporan mecanismos de vigilancia dedicados al tratamiento de datos personales.

En segundo lugar, se insta a las empresas a mantener el llamado Control de las Cláusulas contractuales en la cadena del suministro, lo cual no es mas que ser conscientes de los medios técnicos por los que se hace llegar a la población la publicidad sobre sus productos y servicios, ya que sería posible incorporar programas espía a un software legal con el fin de acceder a datos sensibles, tales como los relativos a la tarjeta de crédito, a documentos confidenciales, etc. Para ello, es de suma importancia que estas empresas comprendan la cadena de relaciones de la contratación, vigilen el cumplimiento de la legalidad y hagan de las prácticas maliciosas de sus contratistas o distribuidores, un motivo suficiente para poner término a los contratos, a través de toda la cadena, de manera que pueda ponerse fin de inmediato a toda relación con las empresas responsables de tales prácticas.

Finalmente, propone a los proveedores de servicios de correo electrónico, a aplicar una política de filtrado que garantice el cumplimiento de la recomendación y de las orientaciones sobre filtrado del correo electrónico, en especial el de salida.

VII.- Medidas respecto de la Comunidad Europea

En primer lugar se señala que la Comisión seguirá abordando los problemas relacionados con el spam, los programas espía y los programas maliciosos en los foros internacionales, en las reuniones bilaterales y, cuando proceda, mediante acuerdos con terceros países, fomentando además la cooperación entre las partes interesadas, incluidos los Estados miembros, las autoridades competentes y la industria.

En segundo lugar, se establece que se adoptarán nuevas iniciativas en los ámbitos de la legislación y la investigación a fin de dar un nuevo impulso a la lucha contra las prácticas maliciosas; al igual que revisará el marco regulador vigente de las comunicaciones electrónicas reforzando la normativa relacionada con la privacidad y la seguridad, proponiéndose desde ya la obligación de los operadores de redes y los proveedores de servicios a:

- notificar a la autoridad competente del Estado miembro cualquier violación de la seguridad que haya ocasionado la pérdida de datos personales y/o la interrupción de la continuidad del suministro del servicio;
- notificar a sus clientes cualquier violación de la seguridad que haya ocasionado la pérdida, modificación o destrucción de sus datos personales, o el acceso a los mismos.

En tercer lugar, la comisión en el desarrollo del Séptimo Programa Marco de la UE, propone proseguir el desarrollo de los conocimientos y tecnologías necesarios para la seguridad de los servicios y sistemas de información, en estrecha coordinación con las iniciativas políticas.

Finalmente, en atención a que Internet es una red mundial, motivo por el cual el compromiso de combatir el spam, los programas espía y los programas maliciosos, debe extenderse a todo el mundo, por lo que hace necesario la Cooperación con los terceros países, ajenos a la UE.

B.- La situación Española en específico

Analizando la situación actual en Europa, daremos un pequeño vistazo a la situación de esta materia en España, ya que pese a estar imbuida en la UE, independientemente ha constituido un referente en especial para América latina.

En cuanto a la legislación aplicable al SPAM, debemos revisar las siguientes normativas:

- Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico LSSI:
- Ley 32/2003 de 4 noviembre General de Telecomunicaciones LGT:
- Ley-Orgánica 10/1995 de noviembre Código Penal Español:
- Ley Orgánica 15/1999 Ley Orgánica de protección de datos de carácter personal,
- En la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) encontramos los artículos 21 y 22[96]

96 Modificados posteriormente por la Ley General de Telecomunicaciones de 4 de noviembre del 2003

relacionados con el correo electrónico. En el primero de ellos, en el número 1[97], se establece la prohibición expresa de realizar comunicaciones comerciales a través de correo electrónico o medios de comunicación equivalentes sin la autorización expresa de los destinatarios de las mismas.

- La Ley General de Telecomunicaciones (LGT) incorpora el número 2[98] a este artículo para adecuarse a la Directiva 2002/58/CE[99], en donde se flexibilizan los requisitos para correos enviados por empresas, restringiendo el primer punto a la no existencia de una relación contractual previa. Además, en el artículo 22[100] se impone la obligación de las empresas a poner a disposición del usuario una forma fácil y gratuita de darse de baja en la recepción de correos comerciales. Además éstas han de informar a sus clientes de la utilización que se va a hacer de sus datos personales.
- El Código Penal, en su artículo 197[101], contempla la privacidad y la intimidad del correo electrónico, por lo que teniendo en cuenta estas

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

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

99 Directiva 2002/58/CCE. Sobre la intimidad y las comunicaciones electrónicas. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:ES:PDF

100 1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente. A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado. Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.
2. Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito. Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

101 El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

disposiciones la Ley Orgánica de protección de datos es aplicable por extensión al correo electrónico.

Existen otras normas en esta ley, en los que se contemplan una serie de delitos informáticos que, aunque no hacen referencia expresa al correo electrónico, citan que éste es la herramienta utilizada para infringir la ley, tal como ocurre con los artículos 248[102], que trata de las estafas realizadas mediante manipulaciones informáticas, o el 256[103], el que penaliza la utilización de equipos de telecomunicación, como servidores de correo por ejemplo, sin la autorización de su propietario.

El organismo llamado a hacer aplicar en España, LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL, es la Agencia de Protección de Datos (APD o AEPD).

Las funciones y competencias de la Agencia se rigen fundamentalmente por dos leyes. La primera de ellas es la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Esta en su Título VI regula las funciones de la AEPD respecto de la protección de datos, define la figura del Director de la Agencia, marca el carácter del Registro General de Protección de Datos, etc. La segunda ley es la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), la cual entrega a la AEPD competencias específicas en el marco de los ya mencionados artículos 21 y 22, respecto

102 1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero, apropiado exceda de cincuenta mil pesetas. Si se tratara de cosas de valor artístico, histórico, cultural o científico, la pena será de prisión de seis meses a dos años.

103 El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

de las comunicaciones comerciales no solicitadas.

En conformidad a las leyes anteriores la AEPD tiene las siguientes funciones:

a) **Funciones Generales:** Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo al cumplimiento y respeto de los derechos de información, acceso, rectificación, oposición y cancelación de datos.

b) **Competencias en relación con los afectados:** Estas son básicamente:

- Atender sus peticiones y reclamaciones
- Informar de los derechos reconocidos en la Ley
- Promover campañas de difusión a través de los medios de comunicación

c) **En relación con quiénes tratan datos:** Al respecto le compete:

- Emitir autorizaciones previstas en la Ley para poder operar legalmente
- Requerir medidas de corrección
- Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos
- Ejercer la potestad sancionadora
- Recabar ayuda e información que precisen
- Autorizar las transferencias internacionales de datos

d) **En la elaboración de normas:** Sus competencias esencialísimas son:

- Informar acerca de los proyectos de normas de desarrollo de la Ley Orgánica de Protección de Datos.

- Informar acerca de los proyectos de normas que incidan en materias de protección de datos.
- Dictar instrucciones y recomendaciones de adecuación de los tratamientos a la Ley Orgánica de Protección de Datos.
- Dictar recomendaciones en materia de seguridad y control de acceso a los ficheros.

e) **En materia de telecomunicaciones:** Al respecto le corresponde tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo específicamente el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente.

En virtud de estas funciones, la AEPD tiene competencias en el ámbito específico del Spam con contenido comercial, tanto para investigar las denuncias recibidas como para sancionar las posibles infracciones que se encuentren tras el oportuno procedimiento de investigación; pudiendo incluso sancionar directamente a Spammers tanto en España como en el resto de UE, que afecten con sus actividades a usuarios en España.
Las sanciones que puede imponer la AEPD dependen del tipo de abuso y son esencialmente sendas multas que oscilan entre los 30.000 y 600.000 euros.

C.- La experiencia Norteamericana

Para analizar la experiencia norteamericana, deberemos abordarla desde 2 ámbitos, uno la legislación Federal, o sea aplicable a todos los Estados Unidos de Norteamérica, como un todo, y en segundo lugar desde la perspectiva de las leyes estatales, aplicables sólo al Estado emisor.

1.- Leyes Federales

Hasta el año 2003, en Estados Unidos, no existía ninguna ley destinado a regular el SPAM. Con anterioridad se habían presentado diversos proyectos, básicamente a partir de 1999, y de los cuales muchos de ellos fueron recogidos en la llamada **CAN SPAM ACT**.

Dentro de estas normas que merecen especial atención revisaremos brevemente las siguientes:

1.a.- **E-Mail User Protection Act o Ley de Protección del usuario de e-mail**.[104] Esta moción es obra del Senador **Gene Green**, la cual fue presentada el 24 de mayo de 1999, y en virtud del cual se considera ilegal el envío de correos masivos no solicitados ya sea, bajo un remitente falso, una dirección de correo, un número de teléfono, un dominio o cualquier otra información de ruta falsa y la venta o distribución de cualquier tipo de software diseñado para falsificar dicha información. Además, se exigía adicionalmente que los remitentes de este tipo de correo deberán incluir en el contenido de los mismos "cláusulas opt-out".

1.b.- **Inbox Privacy Act of 1999 o Ley de Privacidad de la bandeja de entrada**.[105] Este proyecto fue presentado por los Senadores **Frank H. Murkowski y Torricelli** el 25 de marzo de 1999 y en virtud de el se prohíbe el envío del correo electrónico no solicitado a quien ha elegido no recibir este tipo de mensajes. Para ello, los usuarios que no quieran recibir este tipo de correo electrónico, deben notificar de esta circunstancia a la

104 Disponible para consulta y descarga en http://www.spamlaws.com/federal/summ106.shtml#hr1910. [Fecha de consulta: 23 marzo 2007]

105 Disponible para consulta y descarga en http://www.spamlaws.com/federal/106s759.shtml. [Fecha de consulta: 23 marzo 2007]

Comisión Comercial Federal y a los ISPs. Además, se requiere que los mensajes comerciales de correo electrónico no solicitados, incluyan domicilio físico y virtual (dirección electrónica) del mismo y su número de teléfono. Asimismo deben contener instrucciones para utilizar las cláusulas de opt-out y otra información de ruta que permita identificar claramente al remitente del correo. Por su parte obliga a los ISPs a mantener y hacer pública la lista de clientes que no quieran recibir correo electrónico no solicitado. Por último autoriza a la Comisión Comercial Federal a investigar y hacer cumplir las disposiciones de esta ley.

Este proyecto se encuentra actualmente en la Comisión de Comercio.

1.c.- **Internet Freedom Act o Ley de libertad en Internet**[106], fue presentada por el Senador **Bob Goodlate** el 5 de mayo de 1999. Prohibiría el envío de correo electrónico no solicitado con datos falsos acerca del e-mail del emisor, el nombre de dominio de la empresa o cualquier otra información falsa, así como la distribución del software necesario para falsificar dicha información.

1.d.- **Internet Growth and Development Act of 1999 o Ley de desarrollo y crecimiento de Internet**[107]: Este proyecto fue presentado por el Senador **Rick Boucher** el 5 de mayo de 1999 y convierte en ilegal el uso de los proveedores de servicios para enviar correos comerciales no solicitados a los suscriptores de éstos, en violación de sus políticas. Un proveedor podría demandar a un emisor de estos mensajes sólo si el remitente tiene conocimiento de su política. La Ley también considera ilegal enviar correo comercial no solicitado con dirección u otra información falsa, como asimismo el uso del software que permita falsear

106 Disponible para consulta y descarga en http://www.spamlaws.com/federal/106hr1686.shtml. [Fecha de consulta: 23 marzo 2007]
107 Disponible para consulta y descarga en http://www.spamlaws.com/federal/106hr1685.shtml. [Fecha de consulta: 23 marzo 2007]

la información.

1.e.- **Netizens[108] Protection Act of 1999 o Ley de protección de usuarios de Internet**[109]. Esta moción fue presentada por el Senador **Christopher Smith** el 5 de octubre de 1999 y en virtud de ella se requiere que todos los correos no solicitados contengan el nombre del remitente, la dirección física y electrónica y las cláusulas opt-out. Además, prohíbe que el contenido del asunto o subject en el encabezado del correo sea falso y requiere que los ISPs informen bien a sus usuarios de sus políticas al respecto; ya que sólo de esta manera se encontrarían habilitados para demandar a los remitentes de este tipo de correos en caso de resultar perjudicados.

1.f.- **Protection Against Scams on Seniors Act of 1999 o Ley de Protección de fraudes a personas de la tercera edad**[110]. Este proyecto fue por el Senador **Robert A. Weygand** el 4 de febrero de 1999 y en conjunto con la Telemarketing Fraud and Seniors Protection Act o Ley de Protección de fraudes vía telemarketing a personas de la tercera edad[111], que fuera presentada por el Senador **Ron Wyden** el 24 de marzo de 1999; incluyen disposiciones que autorizan al FTC para regular la publicidad en Internet, incluyendo la transmisión y recepción de los correos comerciales no solicitados, como asimismo una campaña para educar a los jubilados e informar sobre los peligros del fraude del telemarketing y del fraude por Internet. En virtud de estas leyes se extendería el delito de fraude criminal, al fraude realizado vía comunicación Internet. Asimismo ordena a la

108 Termino acuñado por la combinación de "Net" y "Citizen"
109 Disponible para consulta y descarga en http://www.spamlaws.com/federal/106hr3024.shtml. [Fecha de consulta: 23 marzo 2007]
110 Disponible para consulta y descarga en http://www.spamlaws.com/federal/106hr612.shtml. [Fecha de consulta: 23 marzo 2007]
111Disponible para consulta y descarga en http://www.spamlaws.com/federal/106s699.shtml. [Fecha de consulta: 23 marzo 2007]

Comisión Comercial Federal a crear los procedimientos para aplicar las leyes a quienes realicen actos o prácticas engañosas que afecten el comercio de los Estados Unidos en relación con la promoción, anuncio, ofertas para ventas o venta de mercancías o de servicios con el uso de Internet, incluyendo el envío, la transmisión y el recibo de correo electrónico comercial no solicitado.

1.g.- **Wireless Telephone Spam Protection Act of 2001**[112] **o Ley Proteccion de SPAM en comunicaciones telefónicas inalámbricas.** Fue presentada por **Rush Holt** en septiembre de 2000, y es una enmienda a la Ley de Comunicaciones de 1934; y prohibiría el uso de los sistemas inalámbricos para el envío de anuncios no solicitados. El 3 de enero de 2001 pasó por la Comisión de Comercio y Energía.

1.h.- **Unsolicited Comercial Electronic Mail Act of 2000**[113] **o Ley de Correos comerciales no solicitados.** En virtud de esta norma se requeriría que los mensajes de correo electrónico con carácter comercial estuviesen identificados en sus encabezados como tales, con el fin de que los destinatarios puedan identificar los mismos a simple vista utilizando un formato estandarizado que incluya las instrucciones para que el destinatario pueda solicitar volver o no a recibir este tipo de correo (cláusulas:"opt-out"- "opt-in"). Prohibiría la información falsa en la ruta de estos mensajes. También prohibiría la utilización de los recursos de los proveedores de servicios con el fin de enviar correo comercial no solicitado, cuando las políticas de los proveedores de servicios estuviesen claramente expuestas en los sitios web. Este proyecto fue presentado por Heather Wilson el 20 de octubre de 1999 y fue examinado por la Cámara de Representantes del 23 de marzo al 18 de julio de 2000. Luego fue

112 Disponible para consulta y descarga en http://www.spamlaws.com/federal/106hr5300.shtml. [Fecha de consulta: 23 marzo 2007]
113 Disponible para consulta y descarga en http://www.spamlaws.com/federal/hr95.html. [Fecha de consulta: 23 marzo 2007]

complementado por otra versión Unsolicited Comercial Electronic Mail Act of 2001 que lleva la numeración H.R.95, presentado por Gene Green. Este exigía la identificación clara y visible de los mensajes de correo comercial no solicitado. Pero a diferencia del proyecto anterior no requería a los emisores utilizar un formato estandarizado de identificación.

1.i.- **Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000[114].** Este proyecto, junto con el mencionado anteriormente, es el que se convertiría en la conocida CAN SPAM ACT de 2003. Fue presentado por el Senador **Conrad Burns** el 11 de mayo de 2000. Este proyecto requiere que los remitentes de los mensajes comerciales no solicitados, provean a los mismos de la cláusula "opt-out" y que acaten las peticiones de este tipo. Prohíbe el uso de rutas falsas en estos mensajes y prohibiría también la venta o la distribución del software diseñado para falsificar la información de rutas.

Las razones que el Congreso Norteamericano consideró para dictar esta ley, se encuentran especificadas en el epígrafe § 7701. Congressional findings and policy, de la mencionada Ley.

Estas se resumen en las siguientes declaraciones:

1.-Importancia del Correo electrónico como medio de comunicación. El correo electrónico se ha transformado en un medio de comunicación extremadamente importante y popular, tanto con fines personales y comerciales. En este último sentido, su bajo costo y alcance lo hacen muy conveniente y eficiente, ofreciendo oportunidades únicas para el desarrollo

114 Disponible para consulta y descarga en http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]

y crecimiento comercial sin desacuerdos[115].

2.- Resguardo de la eficiencia del correo electrónico. La conveniencia y eficiencia del correo electrónico está siendo amenazado por el crecimiento extremadamente rápido en el volumen de correo electrónico comercial no solicitado[116].

3.- Aumento de costos al receptor del correo electrónico. La recepción de correos electrónicos comerciales no solicitados produce costos al receptor quién no puede negarse a aceptar dichos correos[117].

4.- Protección de la confiabilidad del correo electrónico. La recepción de un gran número de mensajes no deseados también disminuye la conveniencia del correo electrónico, reduciendo la confiabilidad y utilidad del sistema, por cuanto se presenta el riesgo que los mensajes de correo electrónico deseados, tanto comerciales como no comerciales se pierdan, pasen por alto o descarten en medio de un gran volumen de mensajes no deseados[118].

5.- Contenido inapropiado del correo electrónico. Muchos correos electrónicos comerciales contienen material que para muchos receptores son de naturaleza vulgar o pornográficos[119].

---

115 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). § 7701. Congressional findings and policy. (A) Findings.(1). Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]
116 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). § 7701. Congressional findings and policy. (A) Findings.(2). Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]
117 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). § 7701. Congressional findings and policy. (A) Findings.(3). Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]
118 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). § 7701. Congressional findings and policy. (A) Findings.(4). Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]
119 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). § 7701. Congressional findings and policy. (A) Findings.(5). Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]

6.- Aumento de costos para ISPs y otras instituciones. El crecimiento de correos electrónicos comerciales no solicitados impone significativos costos monetarios a los proveedores de servicios de acceso Internet, negocios, instituciones educacionales y sin fines de lucro por Internet que transportan y reciben dichos correos, ya que existe un volumen finito de correos que dichos proveedores, negocios e instituciones pueden manejar sin posteriores inversiones en infraestructura[120].

7.- Animo de engaño de emisores. Muchos emisores de correos electrónicos comerciales no deseados disfrazan a propósito la fuente de dicho correo. Asimismo, muchos emisores de correos electrónicos comerciales no solicitados incluyen información engañosa a propósito en la línea referencia o tema del mensaje para inducir al receptor a ver los mensajes.[121]

8.- Consagración del Opt-Out. Mientras algunos emisores de mensajes de correos electrónicos comerciales proporcionan formas simples y confiables para que los receptores rechacen la recepción -"opt-out de los correos electrónicos comerciales provenientes de dichos emisores en el futuro, otros emisores no entregan dicho mecanismo de "opción de salida" o se niegan a cumplir la solicitud de los receptores respecto de no recibir correos electrónicos desde dichos emisores en el futuro o ambos[122].

9.- Homologación de leyes. Muchos Estados han promulgado leyes que

120 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). § 7701. Congressional findings and policy. (A) Findings.(6). Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]
121 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). § 7701. Congressional findings and policy. (A) Findings.(7) y (8). Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]
122 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). § 7701. Congressional findings and policy. (A) Findings.(9). Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]

intentan regular o reducir los correos electrónicos comerciales no solicitados, pero estos estatutos imponen diferentes normas y requerimientos. Como resultado, parecen no haber tenido éxito en abordar los problemas asociados con los correos electrónicos comerciales no solicitados, debido en parte, a que una dirección de correo electrónico no especifica una ubicación geográfica, puede ser extremadamente difícil para negocios respetuosos del derecho, saber con cual de estos dispares estatutos se requiere que cumplan[123]. Los problemas asociados con el rápido crecimiento y abuso de correos electrónicos comerciales no solicitados no pueden ser resueltos solamente por la legislación Federal. El desarrollo y adopción de enfoques tecnológicos y la búsqueda de esfuerzos cooperativos con otros países serán necesarios también.

En cuanto al contenido de esta ley, la podemos resumir en los siguientes puntos:

- Los usuarios que no deseen recibir Spam se inscribirán en una lista para tal efecto.
- Se prohíbe a los propagadores de estos correos que se escondan detrás de identidades falsas o encabezamientos engañosos.
- Los mensajes deben indicar su contenido con abreviaturas en el asunto del correo para que se puedan filtrar con facilidad.
- Se permite a los ESPs (no a los usuarios) establecer acciones legales contra los Spammers
- Se prohíbe recabar direcciones desde sitios web o "adivinar" direcciones mediante combinaciones de nombres conocidos y dominios de uso generalizado.
- El mensaje deberá incluir una dirección física de respuesta

123 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). § 7701. Congressional findings and policy. (A) Findings.(11) y (12). Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=8. [Fecha de consulta: 23 marzo 2007]

localizada en Estados Unidos.

En su votación, la Cámara de Representantes aprobó por unanimidad la legislación, en la que el Senado introdujo pequeñas modificaciones, sin alterar el espíritu de una ley que había sido defendida por ambos partidos, conocedores de su importancia electoral.

La legislación no proscribe por completo las ofertas comerciales a través del correo electrónico, sino que obliga a las empresas a identificarse debidamente y a ofrecer a los consumidores la posibilidad de no volver a ser contactados.

Los correos pornográficos deberán estar claramente etiquetados como tal y los mensajes de texto enviado a los teléfonos móviles estarán prohibidos, a menos que el consumidor los autorice.

Además, esta ley establece la posibilidad, tanto para el receptor afectado, como para el proveedor de servicios, cuyas redes hayan sido utilizadas para cometer estos ilícitos, para accionar civilmente para demandar y obtener sendas indemnizaciones, que establece la ley.

Al ser una legislación federal, esta ley invalida las iniciativas aprobadas previamente en 35 estados, algunas de las cuales, como en el caso de California, prohíben todo contacto no solicitado y da a los consumidores la posibilidad de querellarse directamente contra las empresas que envían "correos basura".

Como consecuencia de la aplicación de la ley CAN-SPAM, durante el primer semestre del 2.004 se han dictaminado diversas sentencias condenatorias y denuncias contra empresas que realizan Spam en EE.UU.

2.- Leyes Estatales

La ley CAN-SPAM tiene por objeto establecer o reemplazar las leyes estatales "anti-spam," pero no obstante ello, los estados pueden aplicar sus propias leyes en preferencia de las secciones de la Ley CAN-SPAM en la medida que cualquiera de sus normas prohíba la falsedad o engaño en todo o parte del mensaje de correo electrónico comercial o información adjunta en el.[124] Así mismo las leyes estatales que prohíben actos fraudulentos o engañosos y delitos por computadora siguen en vigor.

No obstante lo anterior, revisaremos algunas leyes, en atención que su aplicación o no, queda restringido a principios propios de la casuística, de la legislación angloamericana.

2.a.- California

Este Estado aprobó **California Business and Professions Code**[125], el 26 de septiembre de 1998, la cual contemplaba requisitos similares a los establecidos en la actual CAN SPAM ACT, por el cual los mensajes comerciales no solicitados de correo electrónico deben incluir:

- Un número de teléfono gratuito o una dirección de correo electrónico verdaderos para que el receptor notifique que no desea recibir más mensajes no solicitados.
- La información verdadera del remitente.
- Identificación de este tipo de mensajes en el principio de la línea del asunto mediante la incorporación de la leyenda "ADV" como los primeros cuatro caracteres. Además, si se tratare de mensajes con

[124] SEC. 8. EFFECT ON OTHER LAWS. The Can-Spam Act 2003. Disponible para consulta y descarga en: http://www.legalarchiver.org/cs.htm. [Fecha de consulta: 23 marzo 2007]

125 Disponible para consulta y descarga en: http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=17001-18000&file=17529-17529.9. [Fecha de consulta: 23 marzo 2007]

contenido sexual prohibido para menores de edad, debe contener la palabra adulto en el asunto, mediante la incorporación de la leyenda "ADV:ADLT" como los primeros ocho caracteres.

Por otra parte, la ley también se preocupa de proteger al proveedor de servicios de correo electrónico, cuyas políticas respecto de la publicidad no solicitada enviada por correo electrónico sean violadas, de manera que pueda iniciar las acciones civiles pertinentes para reclamar indemnizaciones por los daños y perjuicios sufridos por dicha violación, o una indemnización de cincuenta dólares por cada mensaje de correo electrónico enviado o distribuido en violación de la ley, hasta un máximo de veinticinco mil dólares diarios, correspondiendo aplicar la suma que resulte mayor. Para ello, y como requisito de previo y especial pronunciamiento, se requiere que el proveedor de servicios de correo electrónico previamente a la violación alegada, demuestre haber notificado fehacientemente al demandado sobre sus propias políticas de publicidad no solicitada enviada por correo electrónico.

2.b.-Colorado

Este Estado aprobó la **Colorado Junk Email Law** o Ley del estado de Colorado en materia de Correo electrónico comercial no solicitado[126] el 3 de junio de 2000.

Esta ley prohíbe el envío de mensajes de correo electrónico comercial no solicitado que no revele la dirección real del remitente de dicho correo, como asimismo cualquier información falsa sobre el encaminamiento del

126 Disponible para consulta y descarga en:http://www.ago.state.co.us/FAQ/junk_email_FAQ.cfm. [Fecha de consulta: 23 marzo 2007]

mensaje, o la utilización de una dirección de Internet o el nombre de dominio de un tercero sin el consentimiento de éste.

Igualmente introduce la obligación de identificar estos mensajes, en el asunto excepto cuando:

- Se trate de una organización que utiliza el correo electrónico exclusivamente para comunicarse con sus miembros
- Se trate de una organización que utilice el correo electrónico para comunicarse exclusivamente con sus empleados o contratistas, o ambos

Cuando exista una relación comercial actual o anterior con el receptor del mensaje. A fin de evitar interpretaciones esta misma ley se encarga de dar el significado de "relación comercial actual o anterior" , diciendo que es cuando: a) el receptor ha manifestado su deseo de recibir mensajes de correo electrónico comerciales de ese remitente, b) el receptor ha adquirido o alquilado inmuebles, muebles o servicios al remitente del mensaje de correo electrónico comercial no solicitado, el mensaje enviado por el remitente está relacionado directamente con la compra o alquiler y el mensaje es enviado dentro del periodo de garantía o dentro de los 13 meses contados a partir de la fecha de compra o alquiler, el periodo de tiempo que sea de mayor extensión; c) el receptor posee un contrato vigente con el remitente del mensaje de correo electrónico comercial no solicitado y el mensaje del remitente está relacionado de manera directa con el contrato vigente.

Al igual que la ley anterior, prohíbe el envío de mensaje de correo electrónico comercial no solicitado que no provea un mecanismo del tipo OPT_OUT.

Por último, también establece la posibilidad de iniciar acciones civiles por daños y perjuicios contra quién viole sus disposiciones, tanto por parte del receptor afectado, como por todo proveedor de servicios de correo electrónico cuya red o facilidades hayan sido utilizadas en la transmisión o en la tentativa de transmitir un mensaje de correo electrónico comercial no solicitado.

2.c.- Idaho

Este Estado aprobó el 17 de abril de 2000, la **Unfair Bulk Electronic Mail Advertisement Practices**[127] o **Prácticas desleales relacionadas con la publicidad masiva por correo electrónico**; la cual contiene disposiciones sobre las prácticas desleales relacionadas con la publicidad masiva por correo electrónico. Dispone que toda persona que utilice un servicio informático interactivo para iniciar o causar el envío o la transmisión de cualquier publicidad masiva por correo electrónico, deberá proporcionar una dirección de correo electrónico que se pueda identificar fácilmente, a la cual el receptor pueda enviar un pedido para que no le remitan más dicha correspondencia.

Esta ley sanciona como ilegal:

- El uso de nombre real o de fantasía de un tercero en la dirección de respuesta sin permiso del tercero, al enviar o transmitir cualquier publicidad masiva por correo electrónico
- Falsear cualquier información que posibilite identificar el punto de origen del recorrido de la transmisión del correo masivo de

127 Disponible para consulta y descarga en: http://www3.state.id.us/idstat/480060003E.K. [Fecha de consulta: 23 marzo 2007]

publicidad

- La falta de información que permita identificar el punto de origen del recorrido de la transmisión de correo electrónico masivo de publicidad
- Enviar o trasmitir publicidad masiva por correo electrónico, transcurrido 5 días desde que el receptor haya solicitado que no se le envíe dicha publicidad

Esta ley también otorga acciones civiles al receptor, y permite legalmente a los responsables del servicio informático no responder por el bloqueo o acción de impedir la recepción o la transmisión de cualquier publicidad masiva a través de su sistema que pueda considerarse, de manera razonable, que viola las disposiciones de la ley.

2.d.- Nevada[128]

Este Estado a través de la **Liability of Persons who Transmit Items of Electronic Mail That Include Advertisements**[129], regula la Responsabilidad de las personas que transmiten mensajes de correo electrónico que incluye publicidad; señalando que quien transmite a un receptor un mensaje de correo electrónico que incluya publicidad o causa dicha transmisión, es responsable por los daños y perjuicios causados al receptor, salvo que:

- El receptor haya aceptado expresamente recibir el mensaje o el mismo sea obtenido en forma voluntaria a través de un bulletin board electrónico.
- La publicidad sea fácilmente identificable como promocional o

128 Nevada fue el primer Estado que decretó la legislación del Spam.-
129 Disponible para consulta y descarga en: http://www.spamlaws.com/state/nv.shtml. [Fecha de consulta: 23 marzo 2007]

> contenga una frase que aclare que se trata de publicidad y además en forma clara y visible contenga también el nombre legal, el domicilio completo y la dirección de correo electrónico del emisor, con instrucciones para que el receptor pueda optar por no recibir mas dichos mensajes.

El receptor al igual que en las leyes anteriores podrá reclamar una indemnización por los daños y perjuicios ocasionados.

Se exime de responsabilidad a los proveedores de acceso a la red que, como parte de dicho servicio transmita mensajes de correo electrónico en nombre de los usuarios, a menos que incluya publicidad que el proveedor haya preparado o haya hecho preparar.

2.e.- Lousiana

El Estado de Lousiana[130] considera ilegal el uso de una computadora, una red informática o de los servicios informáticos de un proveedor de servicios de correo electrónico para la transmisión de correo electrónico masivo no solicitado, sin autorización o violando las políticas establecidas por el proveedor de servicios de correo electrónico.

No considera como correo electrónico masivo no solicitado, el realizado por parte de una organización a sus miembros, ni la transmisión de correo electrónico no comercial.

Además esta norma prohíbe expresamente:

130 Titulo 14 derecho penal Articulo 73.1 Modificado por Ley 1180. Aprobado por el Gobernador 9 de julio de 1999, fecha de entrada en vigencia: 15 de agosto de 1999.- Disponible en: http://www.spamlaws.com/state/la.shtml. [Fecha de consulta: 23 marzo 2007]

- El uso de una computadora o una red informática sin permiso, con la intención de falsificar o adulterar de cualquier modo información referente a la transmisión de correo electrónico u otra información referente al encaminamiento de esté relacionada con la transmisión de correo electrónico masivo no solicitado.
- La venta o distribución de software diseñado o producido con el fin de facilitar o posibilitar la falsificación de información relacionada con la transmisión de correo electrónico u otra información relacionada con el encaminamiento.

2.f.- Washington

Este Estado prohíbe el correo electrónico no solicitado o engañoso en términos similares a la actual CAN SPAM ACT[131].

También establece indemnizaciones tanto a favor del receptor del SPAM, como del proveedor del servicio de correo electrónico.

Establece que constituye una violación a la ley de protección al consumidor, ayudar en la transmisión de un mensaje de correo electrónico comercial, sabiendo o evitando conscientemente saber, que quien origina el mensaje de correo electrónico comercial está involucrado, o tiene intención de involucrarse en cualquier acto o práctica que viole la ley de protección al consumidor.

Finalmente dispone el derecho del proveedor del servicio de correo electrónico a bloquear la recepción y/o transmisión de cualquier correo electrónico comercial que considere razonablemente que es o será enviado

131Disponible para consulta y descarga en: http://www.spamlaws.com/state/wa.shtml. [Fecha de consulta: 23 marzo 2007]

violando las disposiciones citadas.

2.g.- Connecticut

El 23 de junio de 1999 se aprobó la ley **An Act Prohibiting Unauthorized Use of a Computer and Other Computer Offenses**[132] que prohíbe el uso no autorizado de una computadora y otros delitos informáticos.

Al respecto:

- considera ilegal que una persona utilice una computadora o red informática sin autorización y con la finalidad de adulterar o falsificar información referente a la transmisión de correo electrónico u otra información referente al encadenamiento que esté relacionada con la transmisión de correo electrónico masivo no solicitado a través de una red informática o hacia una red informática de un proveedor de servicios de correo electrónico o a sus abonados.
- prohíbe la venta y distribución de software diseñados o producido con el fin de facilitar o posibilitar la falsificación de información relacionada con la transmisión de correo electrónico u otra información relacionada con el encadenamiento del tráfico.
- El receptor puede demandar por los daños y perjuicios ocasionados, sólo al spammer, no al proveedor de servicio de correo electrónico, que simplemente transmita el correo a través de su red informática; o puede optar por percibir la suma de diez dólares por cada uno de los mensajes de correo electrónico masivo no solicitado o la suma de veinticinco mil dólares diarios, correspondiendo aplicar la que resulte menor, además de los honorarios de los abogados y las

132 Disponible para consulta y descarga en: http://www.spamlaws.com/state/ct.shtml. [Fecha de consulta: 23 marzo 2007]

costas del juicio.

- el proveedor de servicios, éste tiene la misma opción señalada en el punto anterior respecto del spamer,
- fija la prescripción de la acción civil en el plazo de dos años a contar desde el momento en que se cometió el acto.

2.h.- Delaware

La legislación aprobada el 23 de junio de 1999, incorporó a su ley penal los artículos 937 y 938[133], por los cuales dispone que una persona será culpable del delito informático de enviar correo electrónico no solicitado o no autorizado cuando lo haga:

- Sin autorización, intencionalmente o imprudentemente distribuya correo electrónico comercial masivo no solicitado.
- Se utilice una computadora o red informática sin permiso con la intención de falsificar o adulterar de algún modo la información referente a la transmisión del correo electrónico masivo no solicitado.
- Venda, dé o distribuya software diseñado o producido para facilitar o posibilitar la falsificación de información relacionada con la transmisión de correo electrónico u otra información relacionada con el encaminamiento.
- No interrumpa rápidamente el envío de comunicaciones electrónicas comerciales cuando así se lo hayan solicitado. Disponiendo además que todo correo electrónico comercial deberá contener instrucciones para que el destinatario pueda solicitar al remitente la suspensión o interrupción de mensajes de correo electrónico comercial.

133 Disponible para consulta y descarga en: http://www.spamlaws.com/state/de.shtml. [Fecha de consulta: 23 marzo 2007]

Por su parte, establece que no se considerarán culpables de delito informático:

- Cuando el receptor haya solicitado la información enviada.
- Cuando la comunicación se efectúe entre una organización y sus miembros.
- Cuando exista una relación comercial preexistente.

Por último esta ley exime de responsabilidad al proveedor de servicios por bloquear la recepción o la transmisión de correo electrónico masivo no solicitado que se efectúe a través de su servicio, siempre que considere que el correo es o será enviado violando las disposiciones citadas precedentemente, o desconecte el servicio que le brinda a quien viole la citada ley.

2.i.- Iowa

El 26 de mayo de 1999[134], este Estado aprobó la legislación por la cual se prohíbe el envío de correo electrónico masivo que cumpla alguna de las siguientes características:

- Se utilice el nombre de un tercero como domicilio electrónico de respuesta, sin el permiso del tercero.
- Se falsee alguna información respecto de la identificación del punto de origen del trayecto de transmisión del mensaje de correo electrónico.

134 Disponible para consulta y descarga en: http://www.spamlaws.com/state/ia.shtml. [Fecha de consulta: 23 marzo 2007]

- No se incluya información que permita identificar el punto de origen o el trayecto de transmisión.
- Cuando se trate de publicidad no solicitada, no contenga una dirección de correo electrónico para que el receptor pueda solicitar que no le envíen más publicidad.
- Continuar con el envío de publicidad no solicitada aun con posterioridad a los 5 días de haber recibido del receptor el pedido de suspensión del envío de este tipo de correo.

Por su parte no considera como correo electrónico comercial no solicitado a los efectos de esta ley, al enviado por una organización a sus miembros o a una organización similar, ni a aquellos a los que el receptor accede a través de un **BULLETIN BOARD**[135] o **BBS** electrónico.

Al igual que las otras leyes otorga acción civil al proveedor del servicio informático interactivo, cuando hayan sido utilizadas sus facilidades sin autorización. Esta ley considera que una persona no tiene autorización cuando utiliza los servicios informáticos de un proveedor de servicios de correo electrónico para transmitir correo electrónico masivo no solicitado en contravención de la autorización que le fuera otorgada o en violación de las políticas establecidas por el proveedor de servicios de correo electrónico, siempre que previamente haya sido notificado fehacientemente de dichas políticas.

Por su parte, el receptor tiene el derecho de solicitar al tribunal competente que prohíba al demandado transmitir al receptor todo tipo de mensajes de correo electrónico que incluyan publicidad.

---

135 Un BBS o Bulletin Board System (Sistema de Tablón de Anuncios) es un software para redes de computadoras que permite a los usuarios conectarse al sistema a través de internet o de una línea telefónica, utilizando un programa, que permite realizar funciones tales como descargar software y datos, leer noticias, intercambiar mensajes con otros usuarios, disfrutar de juegos en línea, leer los boletines, etc.

Por último merece especial comentario las excepciones a esta ley, no constituyéndose la figura típica:

- Cuando un proveedor de servicio transmite correo electrónico en nombre de sus usuarios como parte del servicio de acceso a la red informática.
- Cuando la condición de un proveedor de acceso gratuito a un servicio de correo electrónico sea que los usuarios reciban publicidad no solicitada.
- El proveedor del servicio informático interactivo no es responsable por un acto llevado a cabo voluntariamente y de buena fe para bloquear o impedir la recepción y la transmisión de todo mensaje de correo electrónico comercial realizada a través de sus sistema, y que pueda considerar de manera razonable que viola la ley.

2.j.- Illinois

El Estado de Illinois aprobó su legislación el 22 de julio de 1999[136] por la cual considera ilegal enviar mensajes de correo electrónico comerciales no solicitado, en términos bastante semejante a lo establecido en los otros Estados.

Merece especial comentario el hecho, de que esta ley considera que una persona que falsea o falsifica cualquier información referente al encaminamiento de un correo electrónico masivo no solicitado, comete el delito de manipulación informática.

136 Disponible para consulta y descarga en: http://www.spamlaws.com/state/il.shtml. [Fecha de consulta: 23 marzo 2007]

2.k.- Missouri

El Estado de Missouri el 27 de junio del 2000[137] dictó una ley por la cual los mensajes de correo electrónico comerciales no solicitados deben contener la información de contacto, es decir, número telefónico gratuito o una dirección de correo electrónica válida y las instrucciones para que el receptor pueda solicitar que no le envíen mas este tipo de mensajes.

Esta ley considera una práctica comercial ilegal ayudar en la transmisión de un mensaje de correo electrónico comercial cuando quien provee la ayuda sabe o conscientemente evita saber que quien inició el mensaje participa o tiene la intención de participar en un acto o práctica que viola la ley.

2.l.- Carolina del Norte

Este Estado aprobó el 25 de junio de 1999[138] la legislación por la cual se prohíbe la identificación falsa con la intención de engañar o estafar al receptor o de falsificar de cualquier modo, información referente a la transmisión de correo electrónico comercial u otra información referente al encaminamiento que esté relacionada con la transmisión de correo electrónico comercial masivo no solicitado a través de una red informática o hacia una red informática de un proveedor de servicios de correo electrónico o sus abonados. A quien viola esta disposición se lo considera culpable del delito de intrusión informática, agravándose la pena en relación con los daños causados.

137 Disponible para consulta y descarga en: http://www.spamlaws.com/state/mo.shtml. [Fecha de consulta: 23 marzo 2007]
138 Disponible para consulta y descarga en: http://www.spamlaws.com/state/nc.shtml. [Fecha de consulta: 23 marzo 2007]

2.m.- Pennsylvania

El estado de Pennsylvania en su legislación aprobada el 13 de junio del 2000, que introduce modificaciones al Titulo 18 (Delitos Penales) de las Leyes Consolidadas del Estado[139], considera a Internet como un medio cada vez más valioso para la comunicación que los niños usan con fines de esparcimiento y educación, teniendo muchos de ellos acceso a cuentas de correo electrónico, debiendo por tanto protegerlos de los materiales sobre sexo explicito que se comercializan a través de los mensajes no solicitados de correo electrónico; por lo que se dispone que los mensajes comerciales no solicitados de correo electrónico con contenido sexual explícito deberán llevar la correspondiente identificación al principio del Asunto.

2,n.- Maryland

El Estado de Maryland no ha legislado sobre Spam, y al igual que Arkansas, tiene disposiciones que tratan el hostigamiento por correo electrónico[140] y también sobre publicidad no solicitada a través de fax.

2.ñ.- Tennessee

Este Estado aprobó el 17 de junio de 1999 la legislación[141] que regula la "Publicidad no solicitada enviada por medios electrónicos", por la cual los mensajes de correo electrónico comerciales masivos no solicitados deben incluir:

- Un número telefónico gratuito o una dirección de correo electrónico

139 Disponible para consulta y descarga en: http://www.spamlaws.com/state/pa.shtml. [Fecha de consulta: 23 marzo 2007]
140 http://www.spamlaws.com/state/md.shtml. [Fecha de consulta: 23 marzo 2007]
141 http://www.spamlaws.com/state/tn.shtml. [Fecha de consulta: 23 marzo 2007]

a donde el receptor pueda llamar o enviar un mensaje para notificar que no desea que le sigan mandando documentación no solicitada.

- La información verdadera de contacto.
- La identificación en el Asunto, agregándole asimismo en el mismo si se trata de contenido prohibido para menores "adult".

Por su parte prohíbe:

- La distribución de software diseñado o producido para posibilitar falsificar la información de encaminamiento o cualquier otra requerida.
- El uso sin permiso del proveedor del servicio, cuando éste lo haya prohibido expresamente.
- El envío de correo electrónico una vez recibida la notificación del receptor en la que solicita no recibir mas documentación no solicitada.
- Finalmente, establece acciones civiles, tanto para el receptor y proveedor de servicio afectado, y exime de responsabilidad a este último frente al receptor por haber enviado el correo y frente al emisor por el bloqueo que pueda realizar.

2.o.- Arkansas

Este Estado no legislo directamente sobre el SPAM, sino que estableció un estatuto que prohíbe el hostigamiento por E-mail[142] .

142 **Unlawful computerized communications.** 5-41-108. (a) A person commits the offense of unlawful computerized communications if, with the purpose to frighten, intimidate, threaten, abuse, or harass another person, the person sends a message: (1) To the other person on an electronic mail or other computerized communication system and in that message threatens to cause physical injury to any person or damage to the property of any person; (2) On an electronic mail or other computerized communication system with the reasonable expectation that the other person will receive the message and in that message threatens to cause physical injury to any person or damage to the property of any person; (3) To another person on an electronic mail or other computerized communication system and in that message uses any obscene, lewd, or profane language; or (4) On an electronic mail or other computerized communication system with the reasonable expectation that the other person will receive the message and in that message uses any obscene, lewd, or profane language.

Se establece que una persona comete delito de las comunicaciones, si valiéndose de un computador envía mensajes que tienen por objeto asustar, intimidar, amenazar, abusar o acosar a otra, con causarle daño a ella o a su patrimonio; o se trata de mensajes con lenguaje obsceno o lascivo.

De lo anterior, queda claro que si bien no se trata específicamente de Spam en su concepción usual, sanciona las comunicaciones no deseadas, especialmente cuando sanciona el envío de mensajes obscenos, aun cuando no lleven aparejada la amenaza o intimidación señalada previamente.

Como puede observarse las leyes en comento, de una u otra manera, han establecido sistemas bastante similares para proteger a los receptores del correo electrónico no deseado, en términos bastante coincidentes a la ya mencionada CAN SPAM ACT, con la única excepción, que si bien se establece la posibilidad de que el proveedor de servicios ejerza acciones civiles por los daños, no le exime de responsabilidad por los bloqueos que pudiera realizar, cosa que si establecen la mayoría de los Estados.

D.- Algunas experiencias latinoamericanas

La situación en Latinoamérica no es muy alentadora, existen algunas leyes muy deficientes y unos cuantos proyectos que siendo honestos no

(b) Unlawful computerized communications is a Class A misdemeanor. (c)(1) The judicial officer in a court of competent jurisdiction shall upon pretrial release of the defendant enter an order consistent with Rules 9.3 and 9.4 of the Arkansas Rules of Criminal Procedure and shall give notice to the defendant of penalties contained in Rule 9.5 of the Arkansas Rules of Criminal Procedure. (2) A protective order under subdivision (c)(1) of this section remains in effect during the pendency of any appeal of a conviction under this section. Disponible para consulta y descarga en: http://www.internetlibrary.com/statuteitem.cfm?Num=13. [Fecha de consulta: 23 marzo 2007]

prometen mucho, que demuestran claramente que la Protección de la Intimidad de las personas, no es aún una moneda de cambio valiosa.

Por ello haremos un análisis sucinto al respecto de manera de obtener una visión más compresiva de este problema global.

1.- Argentina

Aún no se ha regulado el tema.

Según la Resolución 338/2001[143], la Secretaría de Comunicaciones ha adoptado un procedimiento para un anteproyecto de ley en relación con el Marco Regulador de Comunicaciones Publicitarias vía correo electrónico. Además, ciertas instituciones y entidades han sido invitadas para colaborar con el anteproyecto de ley, como asociaciones de abogados, compañías de software y universidades, entre otros. Sin embargo, el anteproyecto de ley aún no ha sido promulgado.

No obstante ello, se han presentado condenas por la práctica de Spam. En efecto, una sentencia de Abril de 2006[144] de un Tribunal de Primera Instancia, dictaminó que el spam es ilegal. La causa de esta sentencia fue un caso de habeas data presentado por dos abogados en el año 2003, loc cuales solicitaron que sus datos personales fueran eliminados de la base de datos de la compañía infractora.

Hay que dejar presente, que el recurso de Habeas Data se planteo por la

---

143 Secretaría de Comunicaciones de la República Argentina. [en línea] Resolución S.C. Nº 338/2001 (14/09/2001) Anteproyecto de Ley de Regulación de las Comunicaciones Publicitarias por Correo Electrónico [Fecha de consulta: 28 marzo 2007] Actualización permanente. Disponible en: http://www.secom.gov.ar/municipios/ver.asp?MID=10&tipo=nota&id=128

144 "TANUS GUSTAVO DANIEL Y OTRO c/ COSA CARLOS ALBERTO Y OTRO s/ HABEAS DATA", Expte. n° 1.791/2003. Blog del Foro de habeas Data. [en línea] [Fecha de consulta: 28 marzo 2007] Disponible para consulta: http://www.spamlaws.com/federal/summ106.shtml#hr1910

violación a la privacidad que hacía la compañía infractora al remitirles emails y los daños subsecuentes aparejados, que en este caso estaban constituidos por el daño que sufría el computador de tanto borrar estos correos y los eventuales malwares que traían incluidos. Al respecto el señalado fallo señala "***Respecto del daño que los actores alegan que les origina la recepción del mentado correo masivo no solicitado, ya sea por el costo económico como por el tiempo que esa actividad insume, debe estarse a las probanzas adquiridas a ese efecto. En este sentido, los informes producidos a fs. 413/414, 427/428, 447, 450 y 496/499 por las distintas entidades oficiadas y la pericia mencionada precedentemente (punto 6) –no impugnados por las partes (art. 477 del CPCC)-, dan cuenta del significado del término SPAM y del daño que se ocasiona a los receptores de los mensajes atento al tiempo de descarga que requiere identificarlos, seleccionarlos y borrarlos, así como también al incremento en el costo de recepción y procesamiento. Ello genera, además, la necesidad de implementar sistemas para bloquear y, aún lograr, la protección de los virus que pueden dispensar. / Por su parte, el experto explica el proceso de fragmentación que tiene lugar el almacenamiento y la eliminación de archivos y el perjuicio que ello irroga, que se traduce en una notable disminución de la velocidad de almacenamiento y obtención de información. Asimismo, puntualiza que los correos electrónicos son archivos de pequeño tamaño y, consecuentemente, su excesiva grabación y borrado produce una mayor fragmentación del disco rígido de la computadora***"

Si bien, la condena se produjo no por la actividad misma del Spam, debiera constituir un principio para la lucha en contra del spam en Argentina, considerando especialmente que en el primer semestre de 2008, el 96,5% del correo electrónico cursado en Argentina durante el primer

semestre de 2008 fue "spam", informó Sophos, empresa internacional especializada en seguridad informática.[145]

2.- Bolivia

Los operadores de Internet, teléfonos móviles, y otros servicios relacionados son libres de enviar cualquier tipo de información no solicitada por cualquier medio disponible. No hay limitación alguna a este respecto[146].

3.- Brasil

No hay legislación específica. Sin embargo, hay algunos proyectos de ley en el Congreso en relación al tema, y algunas decisiones inconclusas de la corte acerca de la responsabilidad legal de los spammers basadas en ofensas, violación a la privacidad y protección del consumidor[147].

Actualmente, desde el año 2003, se encuentra en tramitación un proyecto de ley, que regula el Spam.

En dicho proyecto, parte en su art. 1 señalando que sólo se consideran para los efectos de la ley, los correos electrónicos originados en Brasil y cuyo destino sean computadores instalados en Brasil, de manera copulativa[148].

---

[145] Sophos. [en línea] [Fecha de consulta: 14 diciembre 2008] Actualización permanente. Disponible en: http://esp.sophos.com/pressoffice/news/articles/2008/07/dirtydozjul08.html

146 Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2006.Pág. 51

147 Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2006.Pág. 55

148 Art. 1º. Para efeitos da presente Lei, consideram-se as mensagens eletrônicas comerciais não solicitadas, originadas no território nacional e destinadas a computadores instalados no país;

Además, define los correos electrónicos comerciales no solicitados, todos aquellos que tengan por finalidad la divulgación de productos y servicios, sean a titulo oneroso o no[149].

Establece un sistema de Opt- Out, prohibiendo desde la solicitud de cesación que se puedan enviar correos al receptor nuevamente[150].

Señala que todo correo de estas características, debe contener:

a. Identificación en cuanto a su naturaleza y finalidad publicitaria
b. Identificación del nombre y dirección del emisor[151]

Además se establece en el art.5[152] que todo usuario de correo electrónico debe tener la facilidad de identificar todo correo y de poder solicitar al proveedor de servicio que bloquee su recepción dentro las 24 horas siguientes, bajo un apremio de multas.

4.- México

Actualmente, no existe una prohibición general en cuanto a comunicaciones no solicitadas.

Desde finales de 2003, la Procuraduría federal de Protección al

149 Art. 2º. Consideram-se mensagens eletrônicas de natureza comerciais aquelas que tenham como finalidade a divulgação de produtos, marcas e empresas ou endereços eletrônicos, ou a oferta de mercadorias ou serviços, a título oneroso ou não
150 Art. 3º. As mensagens de que tratam a presente Lei, poderão ser enviadas uma única vez, proibida a repetição sem prévio e expresso consentimento do destinatário;
151 Art. 4º. É vedado o envio de mensagem eletrônica não solicitada a quem tiver se manifestado contra seu recebimento; Parágrafo único. Toda mensagem comercial deverá conter, de forma clara, identificação quanto a sua natureza e finalidade publicitária, bem como o nome e o endereço do remetente;
152 Art. 5º. Todo usuário do serviço de correio eletrônico deverá dispor de formas hábeis a identificar e bloquear a recepção de mensagens eletrônicas não solicitadas;
I. Os usuários de serviços de correio eletrônico poderão exigir de seu provedor ou do provedor do remetente o bloqueio de mensagens não solicitadas, bastando para tanto a informação do endereço eletrônico do remetente;
II. Os provedores de acesso são obrigados a atenderem à solicitação de que trata o inciso anterior, em prazo não superior a 24 horas de sua efetivação, vedada a cobrança de taxas de qualquer natureza;

Consumidor (PROFECO)[153] colaboró activamente con países miembros del comité de políticas del consumidor (CCP) para la elaboración de un documento titulado: Background Paper on Spam en donde se hace un análisis del problema del spam y trata de esbozar las herramientas legales que posee cada una de las agencias con la finalidad de combatir esta práctica electrónica.

Posteriormente, como resultado de las reformas a la Ley Federal de Protección del Consumidor (LFPC) del 4 de Febrero del 2004[154], la PROFECO reforzó y mejoró el marco jurídico en los siguientes rubros:

- las prácticas de marketing y de publicidad con el objeto de proteger al consumidor de los mensajes no solicitados que constantemente envían empresas de telemarketing y publicidad por correo electrónico;
- la presentación de denuncias por vía electrónica por incumplimiento a las disposiciones de la LFPC, la Ley Federal de Metrología y Normalización, normas oficiales mexicanas y demás disposiciones aplicables; y
- las notificaciones de PROFECO por vía electrónica u otro medio similar previa aceptación por escrito del consumidor.

Las reformas más importantes en materia de prácticas publicitarias y de mercadotecnia se presentaron en los artículos 17, 18 y 18 BIS de la Ley Federal de Protección al Consumidor, relativos a la publicidad que se envía a los consumidores en forma electrónica y el registro público a cargo de la PROFECO sobre los consumidores que no desean recibir dicha información o publicidad por parte de las empresas.

---

[153] PROFECO. [en línea] México. [Fecha de consulta: 28 marzo 2007] Actualización permanente. Disponible en: http://www.profeco.gob.mx/

[154] Disponible para consulta y descarga en: http://www.cddhcu.gob.mx/LeyesBiblio/pdf/113.pdf. [Fecha de consulta: 28 marzo 2007]

Actualmente se encuentra en tramitación un proyecto de Ley Federal que regula el Correo electrónico, y que se encuentra en tramitación desde noviembre de 2004.Este proyecto, básicamente es una adaptación de la CAN SPAM ACT.

No obstante ello, amplía el término Spam no sólo al Correo comercial no solicitado, pues expresamente señala en su art. 3 letra V) señala: Correo electrónico tipo spam:

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

- Publicidad de productos o servicios;
- Contenido político o religioso;
- Juegos o apuestas;
- Contenido pornográfico de todo tipo, o bien conocidos en la Internet como Correos electrónicos tipo "Hoax";
- Comercio sexual;
- Información falsa;
- Sistemas piramidales o cadenas;
- Todo tipo de comunicación tendiente al engaño o al lucro.

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

Por su parte el Art 4., establece lo que no es SPAM en los términos siguientes: No se considera correo electrónico tipo spam, aquél mensaje de

correo electrónico cuyo contenido sea publicidad de productos o servicios, de carácter comercial, político, religioso, juegos, pornográfico, sistemas piramidales o cadenas, o cualquier contenido similar, que sea solicitado expresamente por el receptor hacia el remitente.

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

5.- Perú

El 13 de abril de 2005, fue publicada en Perú la Ley Nº 28.493[155], que regula el uso del correo electrónico comercial no solicitado (Spam), misma que fue aprobada por el Congreso el 17 de marzo de este mismo año. Con ello, Perú toma la delantera a la mayoría de los países latinoamericanos, definiendo acciones concretas en la regulación a nivel nacional del Spam, en este caso a través de un medio legislativo específico.

No se puede negar que la promulgación de esta Ley constituye un trascendental paso a nivel nacional para establecer la necesidad de combatir prácticas nocivas como lo es el Spam y un compromiso del Estado para ello, pero incluso lo es para la acción latinoamericana en el combate a esta práctica nociva cuyos índices de incidencia comienzan a generar serias consecuencias dentro del marco del uso y confianza en las

[155] Diario Oficial El Peruano. Ley Nº 28.493, que regula el uso del Correo electrónico comercial no solicitado (SPAM) [en línea] Perú. [Fecha de consulta: 14 septiembre 2006] Actualización permanente. Disponible en. < http://www.elperuano.com.pe/>

comunicaciones electrónicas, operación de las redes de telecomunicaciones y el comercio electrónico.

La Ley cumple con el importante elemento de instrumentar definiciones en materia de correo electrónico, entre otros, lo cual es innegablemente útil, sin embargo no cumple con el esencial objetivo que representaría para esta Ley el definir el concepto de "no solicitado" empleado como elemento a regular de acuerdo con el título otorgado a esta ley.

Por otra parte; el artículo tercero consagra el derecho del usuario para rechazar o no la recepción de correos electrónicos no solicitados, pero no se establece el como realizar ese rechazo.

El establecer la responsabilidad de los proveedores del servicio a utilizar medios de filtrado de correo, ya es una carga que normalmente los ISP's ya tienen considerada, pero además se les hace civilmente responsable de los Spam que se envíen a través de sus redes, sin especificar bajo que condiciones, ni se le da la eximente de responsabilidad por bloquear correos.

En el ámbito de la responsabilidad, en el texto del artículo 7 resulta sumamente riesgoso el hacer responsables a las empresas o personas beneficiarias de manera directa con la publicidad difundida, ya que no se contemplan la totalidad de prácticas y objetivos bajo los cuales se genera el spam, contemplando sólo el de carácter comercial y sin considerar que un emisor sin consentimiento puede enviar correos electrónicos a nombre de un tercero, generándole responsabilidad por conductas en las que no participó, o que el fin no sea comercial.

Otra característica de esta Ley, es que deja la idea de que no todo el spam

es ilícito, definiendo las bases para su diferenciación, en la definición del mismo contenida en el art. 2 letra b).

Un elemento interesante es que entrega acciones al receptor para reclamar y exigir al emisor o al proveedor de servicios que le resarza los perjuicios que dicha actividad le acarreó, lo cual al menos coloca al spammer en una situación de que ya no es necesariamente una actividad de bajo costo.

6.- Ecuador

En Ecuador encontramos unos pequeños atisbos de regulación, casi perdidos en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, No. 67[156], publicada el 17 de Abril del 2002. Esta en su capítulo III, al establecer los Derechos de los Usuarios o Consumidores de Servicios Electrónicos, establece en su art. 48, que en forma previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente, sobre los equipos y programas que requiere para acceder a dichos registros o mensajes.

Agrega, que el usuario o consumidor, al otorgar o confirmar electrónicamente su consentimiento, debe demostrar razonablemente que puede acceder a la información objeto de su consentimiento.

Si con posterioridad al consentimiento del consumidor o usuario existen cambios de cualquier tipo, incluidos cambios en equipos, programas o procedimientos, necesarios para mantener o acceder a registros o mensajes electrónicos, de forma que exista el riesgo de que el consumidor

[156] CONATEL. [en línea] Ecuador [Fecha de consulta: 28 marzo 2008] Actualización permanente. Disponible en: http://www.conatel.gov.ec/site_conatel/index.php?option=com_content&view=article&catid=48:normas-del-sector&id=98:ley-de-comercio-electronico-firmas-electronicas-y-mensajes-de-datos&Itemid=103

o usuario no sea capaz de acceder o retener un registro electrónico o mensaje de datos sobre los que hubiera otorgado su consentimiento, se le deberá proporcionar de forma clara, precisa y satisfactoria la información necesaria para realizar estos cambios, y se le informará sobre su derecho a retirar el consentimiento previamente otorgado sin la imposición de ninguna condición, costo alguno o consecuencias. En el caso de que estas modificaciones afecten los derechos del consumidor o usuario, se le deberán proporcionar los medios necesarios para evitarle perjuicios, hasta la terminación del contrato o acuerdo que motivó su consentimiento previo.

El art. 50, inciso 5º establece que en el envío periódico de mensajes de datos con información de cualquier tipo, en forma individual o a través de listas de correo, directamente o mediante cadenas de mensajes, el emisor de los mismos deberá proporcionar medios expeditos para que el destinatario, en cualquier tiempo, pueda confirmar su suscripción o solicitar su exclusión de las listas, cadenas de mensajes o bases de datos, en las cuales se halle inscrito y que ocasionen el envío de los mensajes de datos referidos.

La solicitud de exclusión es vinculante para el emisor desde el momento de la recepción de la misma. La persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se sancionará de acuerdo a lo dispuesto en la ley en comento.

El usuario de redes electrónicas, podrá optar o no por la recepción de mensajes de datos que, en forma periódica, sean enviados con la finalidad de informar sobre productos o servicios de cualquier tipo.

E.- Experiencias asiáticas

En cuanto a Asia, no existe una uniformidad en su regulación, al respecto las distintas experiencias, nos demuestran regulaciones bastante dispares del mundo occidental en general.

1.- China

En Febrero de 2006, el Ministerio de información de la industria (MII) promulgó los Métodos de Servicio Administrativo de Correo Electrónico[157], el cual entró en vigor el 30 de Marzo de 2007. Bajo esta normativa, se prohíbe enviar correo electrónico a direcciones de correo electrónico que son recolectados automáticamente o creadas por sistemas computacionales como los robots o vía cookies o spywares; y enviar correo electrónico que contengan publicidad a los destinatarios quienes no hayan expresamente aceptado recibir dichos correos electrónicos. Quien viole esta prohibición puede estar expuesto a sendas multas.

Además en las ciudades de Beijing y Guangdong se prohíbe absolutamente el correo electrónico no solicitado.

En Beijing, se prohíbe el envío de spam comercial, pero se aplica a servidores ubicados en dicha ciudad, por lo que la norma tiene una aplicación limitada.

En Guangdong, el código que establece las Medidas para la Administración de la Seguridad Pública de los Sistemas de Información Computacional, prohíbe el envío de mensajes no solicitados por cualquier entidad o persona. Así como las normativas de Beijing, las Medidas de Guangdong tienen una aplicación

[157] Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2006.Pág. 102

limitada, ya que sólo se aplican a los remitentes de mensajes no solicitados con base en Guangdong.

2.- Hong Kong

Según se informa en el Boletín del año 2008, de Telecoms and Media[158]; en mayo de 2007, Hong Kong promulgó la Ordenanza de mensajes electrónicos no solicitados[159] (UEMO) así como el Reglamento de mensajes electrónicos no solicitados[160] (UEMR). Con el fin de proporcionar orientación práctica respecto de la solicitud o el funcionamiento de las disposiciones de la UEMO, el Gobierno publicó un código de prácticas, jurídicamente no vinculante en noviembre de 2007.

La implementación de la UEMO, que se llevó a cabo en dos fases separadas, regula todos los mensajes de publicidad o promoción de bienes, servicios, instalaciones, enviados por medios electrónicos, como pre-grabados, tales como mensajes de voz, faxes, e-mails y mensajes a través de los servicios de mensajería corta (SMS) o los servicios de mensajería multimedia (MMS).

La UEMO se aplica extraterritorialmente y regula todos los mensajes electrónicos comerciales que hagan referencia a un link o enlace de Hong Kong, incluyendo cualquier mensaje enviado a Hong Kong, a un número de teléfono de Hong Kong, o enviado o autorizado por una persona natural o jurídica en Hong Kong.

[158] Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2006.Pág. 187
[159] Unsolicited Electronic Messages Ordinance
[160] Unsolicited Electronic Messages Regulation

La primera fase, que entró en vigencia el 1 de junio de 2007, cubre el uso inadecuado de técnicas para comunicarse con varios destinatarios, tales como el suministro de listas de direcciones de correo electrónico para enviar mensajes electrónicos comerciales sin el consentimiento de los beneficiarios, así como de otros tales como la cosecha automatizada de direcciones de correo. La pena máxima para esos delitos es una multa de HK$[161] 1 millón y prisión de hasta cinco años.

La UEMO también prohíbe otras actividades fraudulentas e ilícitas relacionadas con el envío de múltiples mensajes electrónicos comerciales. Una persona que a sabiendas inicia la transmisión de múltiples mensajes electrónicos comerciales arriesga penas de multa y prisión de hasta por 10 años.

La segunda fase, que entró en vigencia el 22 de diciembre de 2007, se refiere principalmente a las normas para el envío de mensajes electrónicos comerciales. Se prohíbe el envío de mensajes, en que el receptor no tenga como solicitar su remoción. Los usuarios que no deseen recibir mensajes electrónicos no consentidas que contengan comunicaciones comerciales no solicitadas, así como llamados telefónicos, debían antes de mayo del año en curso, registrar su teléfono o fax en el número tres do-not-call al (DNC); quedando expuesto los emisores que no respeten dichas solicitudes a sendas multas de HK$ 100.000 en la primera condena y hasta HK$ 500.000 por cada reiteración.

Por otra parte es importante señalar, que la ley de Protección de Datos, incluye como dato sensible de protección las direcciones de correo electrónico en la medida en que contengan el nombre de la persona.

[161] Moneda oficial Dólar de Hong Kong

3.- India

Telecoms and Media 2008[162], informa que no existe ninguna ley que prohíba las comunicaciones electrónicas no deseadas. Sin embargo, prohíbe cualquier comunicación electrónica, cuyo contenido sea obsceno.
Por otra parte la Corte Suprema de la India, decreto en un juicio que las llamadas no solicitadas por motivos de telemarketing, violaban el derecho a la privacidad de las personas, consagrado en la Constitución política de la India, e instruyo al Gobierno a fin de que adopte los procedimientos necesarios para efectuar los bloqueos respectivos.
El año 2007 la TRAI[163] reglamento la creación de un registro de usuarios a fin de que soliciten no recibir llamadas no solicitadas.

4.- Indonesia

No existe en Indonesia, ninguna ley que sancione las comunicaciones electrónicas no solicitas, ya sea por correo electrónico o por SMS. No obstante ello, por aplicación del artículo 1365 del Código Civil, las comunicaciones electrónicas no solicitadas, pueden ser consideradas como un acto ilícito, sujeto a las indemnizaciones que establece dicha norma[164].

5.- Japón

Los correos electrónicos no solicitados están regulados por la Ley sobre Transmisión de Correo electrónicos y la Ley de transacciones

[162] Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2006.Pág. 192
[163] Telecom Regulatory Authority of India
[164] Telecoms and Media 2006. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2006.Pág. 196

comerciales[165]. Estas leyes entraron en vigencia el año 2002,y requieren que los remitentes de correo electrónicos publicitarios se identifiquen como tal, para que el receptor sepa cual es su origen, de manera que a su vez, pueda solicitar y prohibir el envío de correo electrónicos. La sanción en caso de incumplimiento van desde multas hasta la prisión del representante legal.
El año 2007, Japón en lo que respecta a la formalidad para recibir las comunicaciones no solicitadas, cambio del sistema opt-out a un opt-in.

6.- Corea

El artículo 50 de la ley para la Promoción de la utilización de red de comunicaciones e información y protección de la información, prohíbe que cualquier persona envié correo o comunicaciones no solicitadas sin la autorización previa del receptor. Quien incumpla dicha ley, puede ser condenado al pago de 30 millones de wones, es decir, cerca de 33 mil dólares.

7.- Malasia

Hasta el año 2007, según informa "Telecom and Media"[166], no existía ninguna ley que prohibiera las comunicaciones electrónicas no solicitadas.

No obstante ello, la ley sanciona todas las comunicaciones cuyo contenido sea indecente, obsceno, falso, amenazador o de carácter ofensivo con la intención de molestar, abusar, amenazar o acosar a cualquier persona.

---

[165] Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2006.Pág. 227
[166] Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2008.Pág. 270

La ley también establece que cualquier persona que a través de Internet o cualquier red a sabiendas hace, crea o solicita e inicia la transmisión de las comunicaciones de estas características con la intención de molestar comete delito. También comete delito quien inicie una comunicación continuamente, en repetidas ocasiones aun cuando la comunicación puede o no dar lugar, con o sin revelar su identidad y con la intención de molestar.

Si bien la legislación de Malasia no habla de Spam, sanciona a toda persona que envíen mensajes no solicitados, ya sea vía correo electrónico, mensajes cortos de telefonía móvil (SMS) o vía mensajería instantánea, que no hayan dado su aprobación previamente.

La Comisión Malaya de comunicaciones y multimedia, anuncio el 23 de noviembre de 2007, que se comenzó a realizar un estudio estratégico para revisar las políticas anti-spam con la intención de proporcionar un marco legislativo eficaz, con el fin de proteger a los usuarios e impedir la actividad de los spammers eficazmente.

8.- Singapur

La reciente "Spam Control Act" de 2007 prohíbe enviar de Emails y SMS no solicitados del texto. Tales comunicaciones serán consideradas "Spam" cuando sean de naturaleza comercial; no hayan sido solicitadas por el receptor; hayan sido enviados masivamente y guarden alguna relación con Singapur; requisitos que se explican uno a uno a través de los párrafos 3 a 7[167], de la parte primera de la norma en comento.

[167] Spam Control Act" de 2007. Singapur. [en línea] [Fecha de consulta: 17 diciembre 2008] Actualización permanente. Disponible en: http://statutes.agc.gov.sg/

Los Spammers no serán penalizados si el mensaje contiene una facilidad válida del "unsubscribe" y la comunicación satisface los requisitos de etiquetado (indicar que es anuncio).

Dicha ley tiene por objeto balancear los intereses validos de la industria del telemarketing y los intereses y derechos de los usuarios de no ser invadidos en sus correos electrónicos.

La ley establece que una persona podrá demandar a un Spammer, siempre que este no se excepcione y demuestre que envió la comunicación por error.

Finalmente, también se regula la prohibición de enviar emails fraudulentos, o con publicidad engañosa o remitir pornografía.

9.- Taiwán

Según señala el informe anual de "Telecom and Media 2008"[168]; actualmente no existe ninguna norma que prohíba o regule correo comercial no solicitado en Taiwán. No obstante ello, existe un proyecto para ello, y que exige que el remitente del correo electrónico comercial debe

(i) proporcionar un mecanismo de opt-out,
(ii) identificar el correo electrónico como un anuncio,
(iii) incluir en el subject o asunto un la verdad de sus intenciones

Por último se establece en el marco del proyecto, que los violadores de las

[168] Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2008.Pág. 423

normas anteriores, tendrán responsabilidad civil por daños y perjuicios y responsabilidad penal.

F.- Legislación Africana

Al respecto podemos destacar:

1.- Nigeria

La información respecto de Nigeria y esta regulación, es que si bien no existe ninguna ley que sanciones este tipo de comunicaciones electrónicas; existe un proyecto de ley, que tipifica como delito, toda comunicación electrónica no solicitada, estableciendo penas privativas de libertad bastante altas.[169]

2.- Sudáfrica

Los correos electrónicos no solicitados se encuentran regulados por la **Ley de Comunicaciones y transacciones electrónicas de 2002**; la cual si bien no prohíbe dichas comunicaciones, obliga a los emisores a entregar informaciones a los receptores al envío del correo electrónico, de no hacerlo así, se encuentran afectos a ser condenados por delito[170].

G.- Legislación Australiana

Al respecto, es importe revisar las siguientes experiencias:

---

[169] Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2008.Pág. 311
[170] Telecoms and Media 2008. An overview of regulation in 48 jurisdictions worlwide. Global Competition Review.London 2008.Pág. 389

1.- Australia

La Ley Antispam del 2003[171] prohíbe el envío de spam, lo que se identifica como un mensaje electrónico comercial enviado por correo electrónico, SMS, MMS o mensajería instantánea sin el consentimiento del destinatario. La Ley Antispam también apunta a evitar recolección de direcciones de correo electrónico.

Los requerimientos bajo la Ley Antispam se aplican a todos los mensajes electrónicos comerciales, incluyendo tanto los masivos como los mensajes individuales. La Ley Antispam sólo cubre a los mensajes electrónicos comerciales que tengan un origen australiano. Las excepciones incluyen los facsímiles y llamadas de voz.

Existe una ley, la llamada "Registro de No Llamar" ('Do Not Call Register') de 2006, que permite a las personas con números telefónicos de red fija y celulares registrar sus nombres en un directorio público, si no quieren recibir ciertas llamadas de telemarketing no solicitadas. El Registro está diseñado para proteger la privacidad de las personas y números telefónicos y proporcionar una oportunidad de optar por no recibir llamadas de telemarketing.

2.- Nueva Zelanda

En septiembre de 2007 ha entrado en vigencia la ley de mensajes electrónicos no solicitados[172], que tiene por objeto promover la seguridad y un entorno de mayor protección para la utilización de las tecnologías de la información y las comunicaciones; para disuadir a las personas de utilizar

[171] ttp://www.danacrm.com/wiki/index.php/Reglamentos,_Leyes_y_Legislaciones_Antispam_en_el_mundo
[172] Unsolicited Electronic Messages Act 2007. [en línea] [Fecha de consulta: 17 diciembre 2008] Actualización permanente. Disponible en: http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html

las tecnologías de la información y las comunicaciones indebidamente.

Se define un mensaje electrónico comercial como aquel que promueve los mercados o los bienes, los servicios, la tierra, el interés en la tierra, una oportunidad de inversión o de negocios.

Esta ley sólo prohíbe el envío no solicitado de mensajes electrónicos comerciales, y comprende las casillas de correo electrónico, los SMS y los números telefónicos.

Una persona que alega que el destinatario consintió en recibir un mensaje tiene la carga de la prueba.

Se establece un sistema OPT OUT, de manera que el receptor pueda solicitar el darse de alta sin incurrir en costo alguno.

Por último la ley establece acciones civiles para recurrir en contra de los infractores.

IV.- REGULACION Y EXPERIENCIA CHILENA

Respecto a la reglamentación del Spam, la legislación no es mucho mas feliz que en el resto de Latinoamérica. A la fecha han existido diversos proyectos, que de una u otra manera han tratado de introducir el tema, pero en general no han prosperado, básicamente por falta de información o desconocimiento real del mundo de los servicios de correo electrónico.

En este escenario haremos un estudio respecto de estas iniciativas, en general casi todas fallecidas por muerte natural por abandono, salvo una y la que en definitiva reguló este tema "de pasadita" como diríamos en buen chileno, incorporándola en la Ley de Defensa del Consumidor.

A.- Proyecto Diputados Alberto Espina y Patricio Walter

Este proyecto cuyo objeto era reglamentar una **LEY SOBRE COMUNICACIONES ELECTRÓNICAS**[173], fue presentado el 13 de junio del 2000.

Este proyecto, mas que regular las comunicaciones electrónicas, era un gran cajón de sastre que buscaba regular, todo lo que sonaba a Comercio electrónico e Internet, sin distinguir mayormente entre una materia y otra.

En la exposición de motivos contenida en los antecedentes, nos encontramos con motivos plausibles y originales, tales como la revolución

173 BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 2512-07. [en línea] Chile. [Fecha de consulta: 20 de abril 2007] Actualización permanente. Disponible en: http://www.bcn.cl/

tecnológica, la integración digital, más conocida actualmente como la "convergencia" y la gran aldea global.

Se buscaba proteger y regular temas de índole jurídica, como la propiedad intelectual, muy afectada por la piratería y en especial por que Internet, a juicio de los legisladores y siguiendo al abogado **Renato Jijena**, "las redes han "desmaterializado" las obras creadas por los autores, ya que las creaciones originales digitalizadas se reproducen, circulan y se distribuyen rápida y electrónicamente, sin que se encarnen en un soporte físico concreto o en alguna de las formas envasadas que históricamente han contenido las obras artísticas e intelectuales, haciéndose fácil que sean ilícitamente reproducidas, transformadas y copiadas con fines comerciales o "pirateadas" y sin que exista diferencia alguna entre un original y una copia electrónica"

Se preocupaban además de regular las direcciones Ip y los nombres de dominio, en especial como fuente de conflicto con el mundo marcario.

Por otra parte, y acercándose mas a nuestro interés, pretendían regular la privacidad, toda vez que se señalaba ***"la proliferación del comercio electrónico ha facilitado la creación de grandes bases de datos, con información sobre datos personales de personas físicas o jurídicas, los que fácilmente pueden ser recopilados, procesados, almacenados y cruzados sin autorización de su titular, y ser comercializados, por ejemplo, para realizar marketing directo."***[174] Por ello, se hacía indispensable velar por la adecuada protección de la privacidad de las personas, consagrada en el artículo 19 Nº 4 de la Constitución Política del Estado, fortaleciendo las normas contenidas en la ley Nº 19.628 sobre Protección de la Vida Privada.

[174] BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 2512-07. [en línea] Chile. [Fecha de consulta: 20 de abril 2007] Actualización permanente. Disponible en: http://www.bcn.cl/

Por otra parte, era de su interés dar seguridad a todas las transacciones electrónicas que habían surgido gracias a la proliferación del comercio electrónico en Internet.

Por último se preocupaban de regular los contenidos de Internet, en atención al hecho de la verdadera **"SATANIZACIÓN DE INTERNET**", ***"de que además de los grandes beneficios y progresos que ha permitido Internet, también ha sido un medio empleado para la transmisión de contenidos ilícitos o nocivos, así como también un medio usado para actividades criminales y terroristas."*** Agregando que ***"no obstante la tipificación de estas actividades en muchos países, la naturaleza misma de Internet impide que tales conductas pueden ser perseguidas y sancionadas, salvo que exista un consenso internacional que se plasme en algún tratado."***

Todos estos argumentos llevaron a presentar el proyecto de Ley sobre Comunicaciones Electrónicas[175], que era una elegante mixtura entre el Real Decreto-Ley 14/1999 de España, la ley Nº 527 de 1999 de Colombia y la ley Modelo de la Uncitral; que constaba de de treinta y seis artículos permanentes y tres artículos transitorios, cuya estructura general era:

a) Título Preliminar denominado "Disposiciones Generales", compuesto 5 artículos en los que entre otras cosas se establecía el ámbito de aplicación de la ley; se daban definiciones legales, tales como; firma electrónica, mensaje de datos y prestador de servicios de certificación. Además, se establecía un principio de no discriminación entre el documento y firma electrónica y sus equivalentes en papel; y se entregaba

[175] BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 2512-07. [en línea] Chile. [Fecha de consulta: 20 de abril 2007] Actualización permanente. Disponible en: http://www.bcn.cl/

al Ministerio de Transportes y Telecomunicaciones, a través de la Subsecretaría de Telecomunicaciones, la aplicación y control de la ley y sus reglamentos y la interpretación técnica de las mismas; y por último se consagraba el principio de la neutralidad tecnológica que inspira la ley.

b) Título I denominado Transmisiones Electrónicas, que se dividía en seis secciones:

Sección 1, El "Mensaje de Datos", regulado en cinco artículos, en los que regula el mensaje de datos y su valor probatorio.

Sección 2, "Comunicación de los Mensajes de Datos", regulado en cinco artículos, en los que se regula el envío y recepción de los mensajes de datos, la formación del consentimiento y autoría de los mismos.

Sección 3, "Legislación Aplicable y Jurisdicción", que constaba de un artículo, en el que se regula la legislación aplicable y jurisdicción entre personas con y sin domicilio en el país.

Sección 4, "Propiedad Intelectual", que constaba de dos artículos, en los que se reconocen los bienes digitales, dándoles la protección del derecho de autor y se relacionan los nombres de dominio con las marcas comerciales.

Sección 5, "Contenidos", que constaba de un artículo, en el que se establece las responsabilidades y obligaciones de los prestadores de servicios de transmisión o de servicios de acceso a la red de comunicaciones.

Sección 6, "Privacidad de los Datos", que pretendía en un sólo artículo complementar las disposiciones de la ley Nº 19.628 respecto de la recolección de datos en forma electrónica.

c) Título II denominado "Prestación de Servicios de Certificación", dividido en cuatro secciones:

Sección 1, Normas Generales, que constaba de cuatro artículos, en los que regula la prestación de servicios de certificación, sin exigencia de autorización previa, no obstante exigirse la inscripción en un registro que llevará la Subsecretaría de Telecomunicaciones. Adicionalmente se contempla un sistema voluntario de acreditación.

Sección 2, Certificados, que constaba de dos artículos, en los que se regula el contenido y vigencia de los certificados.

Sección 3, Condiciones Exigibles a los Prestadores de Servicios de Certificación, que constaba de cuatro artículos, en los que se establecen las obligaciones de los certificadores acreditados y no acreditados y su responsabilidad.

Sección 4, Inspección y control de la actividad de los prestadores de servicios de certificación, que constaba de tres artículos, en los que se entrega al Ministerio de Transportes y Telecomunicaciones, a través de la Subsecretaría de Telecomunicaciones, el control y fiscalización del cumplimiento de las obligaciones aplicables a los prestadores de servicios de certificación.

d) Título III denominado "Sanciones", que constaba de tres artículos, en los que se establecen infracciones y el procedimiento aplicable. Asimismo, se tipifican como delitos de acción pública una serie de conductas que afectan la seguridad e integridad de los mensajes de datos y los derechos de los autores sobre obras digitales, reconociéndose una indemnización

legal para el afectado.

e) Título Final que contenía tres disposiciones transitorias, estableciendo los plazos dentro de los cuales deben dictarse los reglamentos previstos en la ley, y una exención temporal en favor de los Notarios que deseen prestar servicios de certificación acreditado.

Este proyecto, en cuanto a la materia que nos interesa, esbozaba una regulación de las comunicaciones electrónicas, llamadas en este proyecto comunicaciones de datos y que atendía mas a aquellas materias relacionadas con la formación del consentimiento en un contrato electrónico, y realmente no consideraba las comunicaciones electrónicas no deseadas. Básicamente podíamos decir que en su utópico mundo, al regular las transacciones electrónicas, regular la firma electrónica y las certificaciones, así como los contenidos y propiedad privada, no había de que preocuparse de la existencia de los correos electrónicos no solicitados.

Este proyecto, con fecha 5 de octubre de 2000 se solicitó por oficio 279-00 que fuera tramitado conjuntamente con el proyecto sobre firma electrónica y los servicios de certificación de firma electrónica, el cual se convirtió en ley, a diferencia de este, el cual fue archivado el 19 de marzo del 2003.

B.- Proyecto Alejandro Navarro

El Proyecto denominado **"SOBRE COMERCIALIZACIÓN Y PUBLICIDAD POR MEDIO DE REDES DE TELECOMUNICACIONES E INTERNET"**[176], vio la luz, al amparo del siempre inspirado diputado **Alejandro Navarro**, hoy Senador de la Republica.

176 BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 3094-19. [en línea] Chile. [Fecha de consulta: 20 de abril 2007] Actualización permanente. Disponible en: http://www.bcn.cl/

En su exposición de motivos, señala el otrora diputado ***"que el avance de las nuevas tecnologías de la información e internet ha traído consigo, a su vez, algunos problemas relacionados, por ejemplo, como la validez de las transacciones electrónicas, el aumento de los delitos de carácter informáticos, el uso autorizado de los contenidos que se entregan a través de internet, el derecho a la privacidad de las personas que navegan por la red, o el uso abusivo o indebido de datos personales y la comercialización y publicidad no autorizada a través de redes de telecomunicaciones y telemáticas, y que afectan a la sociedad en su conjunto y en particular al usuario consumidor de bienes y servicios ofertados a través de las redes informáticas".***

Al respecto cita al entonces director del Servicio Nacional del Consumidor (Sernac), Sr. **Álvaro Undurraga** quien en relación al tema de los correos electrónicos no deseados, señaló que ***"toda transgresión a la legislación debe ser sancionada"; ya que "no es lo mismo que metan un aviso publicitario por debajo de la puerta, a que te saturen tu e-mail con información no requerida, porque en el primer caso basta con arrugar el papel y tirarlo a la basura, pero en el segundo se debe incurrir en pérdidas de tiempo y de recursos".***

Navarro continúa haciendo una relación con la cantidad de internautas a la fecha y de casillas de correo electrónico, y del riesgo de verse infectados por de 100 millones de correos electrónicos de índole comercial o publicitaria, a razón de unos 60 correos por usuario. Ello es el principal problema que lo lleva a regular estas comunicaciones y a buscar una solución.

Además basado, en estudios de la Cámara de Comercio de Santiago (CCS)

asocian el costo -país con pérdida de tiempo laboral y eficiencia monetaria, asociada al desgaste que produce "***bajar***" la información proveniente de correos electrónicos. Señala al respecto que "***la CCS estima que las personas se demoran en torno a un minuto en leer y borrar esta correspondencia, por lo que todo el proceso, desde que es detectado hasta ser eliminado, toma cerca de dos minutos, lo que equivale a tres días laborales al año por persona"***.

Luego de revisar las directivas de la Unión Europea, en especial la diferenciación entre los sistemas de exclusión Out-Pot y Out_In, pasa a analizar la diferencia que existe entre el spamming y prospección no solicitada.

Señala al efecto, que ***"se entiende por spamming el envío masivo y repetido de mensajes comerciales no solicitados procedentes de un remitente que oculta o falsifica su identidad. Desde este punto de vista, constituye, evidentemente, un método de prospección no solicitada. Sin embargo, se distingue por su carácter masivo, repetido y desleal. En una palabra, el spamming constituye prospección comercial no solicitada, pero no toda prospección no solicitada es spamming***". Agrega, que "***en sentido estricto, una comunicación comercial no solicitada tiene dos características: ser comercial y no haber sido solicitada, es decir, reclamada previamente por el internauta. Ahora bien, si la mayoría de los profesionales europeos niega recurrir al spamming, se muestran evasivos, en cambio, sobre su deseo de enviar mensajes no solicitados***".

Luego de un profundo análisis de la manera en que se ha recogido las direcciones electrónicas por los emisores, llega a la conclusión, apoyado por las conclusiones de una reunión internacional celebrada en París del

12 al 15 de septiembre de 2000, que se ha traducido, en Finlandia, en un Código Deontológico del Marketing Directo, que prevé la garantía del consentimiento previo, que la solución pasa por la inclusión voluntaria de los usuarios.

Ello, a su juicio permitía una gestión rentable de las bases de datos de correo electrónico, mantiene la relación personalizada de los comerciantes con los internautas y parece responder a las expectativas de éstos, como se observa en Estados Unidos. Además, da la seguridad de utilizar los datos respetando la voluntad de internauta.

Esta inclusión voluntaria, señala que en caso alguno, prohíbe la prospección comercial de clientes o visitantes. Al contrario, la autoriza. Basta con que la información suministrada al internauta haya sido lo bastante clara sobre este punto. La inclusión voluntaria no prohíbe la cesión a terceros de datos suministrados por los internautas, pero ésta ha de estar subordinada, de conformidad con la Directiva de 1995, a una información previa y al ejercicio del derecho de oposición. La inclusión voluntaria no prohíbe recopilar listas de direcciones electrónicas. Por el contrario, es un elemento central del mercado de los ficheros de prospección comercial y permite su real valorización. La inclusión voluntaria prohíbe la recogida y utilización desleales de los datos y garantiza con ello una protección eficaz de los datos personales, una seguridad jurídica a los comerciantes y un clima de confianza, y permite dejar de oponer artificialmente la protección de los datos personales al comercio electrónico.

Concluyendo, y como considerandos finales, para justificar su proyecto de ley, señalaba:

a.- Se deben establecer salvaguardias para los usuarios de la redes de telecomunicaciones y de internet y cualesquiera otras, que eviten el abuso y uso indebido del sistema de correos electrónicos debido a comunicaciones no solicitadas para propósitos de comercialización, ya sea por medio de ofertas o publicidad de bienes o servicios realizadas por personas o máquinas automatizadas o no, telefaxes u otros sistemas similares de todo tipo. Estas formas de comunicaciones comerciales no solicitadas pueden, de una parte, ser relativamente fáciles de realizar y de bajo costo para enviar, y de la otra pueden imponer una carga y/o un costo al usuario receptor de las mismas.

b.- En algunos casos el volumen puede también causar las dificultades para las redes de comunicaciones electrónicas y el equipo terminal. Sin embargo, el uso de comunicaciones no solicitadas por medio de correos electrónico para la comercialización o publicidad de bienes o servicios puede justificarse si se obtiene el consentimiento explícito anterior del usuario receptor de los mismos, antes que tales comunicaciones se realicen.

c.- Dentro del contexto de una relación existente con un usuario, es razonable permitir el uso de los datos personales de dicho usuario, en la medida que sean de acceso público y que su uso no se torne indebido o abusivo, para el ofrecimiento de bienes o servicios, pero solamente por la misma compañía que ha realizado inicialmente el contacto vía correo electrónico.

d.- Que otras formas de comercialización directa que son más costosas para el remitente y no imponen ningún costo financiero ante los usuarios, tales como telefonía personal de voz, pueden justificar el mantenimiento de un sistema que da a los usuarios la posibilidad para indicar que no desean recibir tales llamadas.

e.- Que para facilitar la aplicación eficaz de estas normativas, es necesario prohibir el uso de identidades falsas, de remitentes o números falsos por parte de quien envía los mensajes no solicitados para los propósitos de la comercialización directa.

f.- Que ciertos sistemas de correo electrónico permiten que los usuarios visualicen la línea del remitente y del tema de un correo electrónico, y también que supriman el mensaje, sin tener que descargar el resto contenido de dicho correo electrónico o cualquier accesorio, de tal modo de reducir los costos que podrían presentarse al descargar correos electrónicos o los accesorios no solicitados.

g.- Que quienes practican el marketing por correo electrónico han descubierto las ventajas comerciales del marketing autorizado, y

h.- Que en muchos países del mundo se han adoptado legislaciones que imponen sanciones penales en este sentido.

En consecuencia de lo anterior, presenta un proyecto de ley que se compone de 2 artículos. El primero contiene dos definiciones, una de correo electrónico y otra de telecomunicaciones, definiendo la primera como "***cualquier mensaje, ya sea de texto, de voz, de sonido o de imagen enviado a través de una red de comunicaciones pública que se pueda almacenar en la red o en el equipo de terminal de un usuario receptor hasta que es recogida por éste***."

El art. 2, Introduce el siguiente párrafo en el Título III "Disposiciones Especiales" de la ley Nº 19.496 que establece normas sobre protección de los derechos de los consumidores, el que pasa a ser el párrafo Nº 6

"Disposiciones relativas comercialización y publicidad por medio de redes de telecomunicaciones. El cual a través de 3 artículos regula "***la comercialización y publicidad de bienes y servicios por medio de redes de telecomunicaciones, utilizando, por ejemplo, alguno de los servicios públicos establecidos en la ley Nº 18.168, ley general de Telecomunicaciones o por medio de la red de internet, utilizando, por ejemplo, los servicios de correos electrónicos; utilizando sistemas automatizados o no, con la intervención humanas o no, se puede permitir solamente en relación a los usuarios consumidores que han dado su consentimiento previo, explícito e inequívoco, en la medida que dicho uso no se torne indebido o abusivo. Los datos deben ser tratados de manera leal y lícita***"[177].

En el Articulo 49 B, propuesto señala que cuando se obtengan datos personales del usuario consumidor por parte de quienes realizan el contacto de la manera señalada anteriormente, este deberá ser informado sobre los fines del tratamiento de que van a ser objeto los datos, su uso posterior para la comercialización y publicidad, los destinatarios o las categorías de destinatarios de los datos, el carácter obligatorio o no de la respuesta, la existencia de derechos de acceso y rectificación de una manera clara, y se le debe dar la oportunidad de rechazar tal uso. Esta oportunidad debe continuar siendo ofrecida con cada contacto posterior, sin excepción.

Agrega, que cuando los datos no hayan sido recabados del usuario, el responsable del tratamiento deberá comunicarle la información desde el momento del registro de los datos o, en caso de que se piense comunicar a un tercero, a más tardar, en el momento de la primera comunicación de datos; de manera que el interesado pueda oponerse costo alguno, por una

177 BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 3094-19. [en línea] Chile. [Fecha de consulta: 20 de abril 2007] Actualización permanente. Disponible en: http://www.bcn.cl/

parte, al tratamiento con fines comerciales de los datos que le conciernan y, por otra parte, a la transmisión de sus datos a terceros, de la que deberá ser informado previamente.

Finalmente establece en el Artículo 49 C, que la comercialización o publicidad realizada de la manera ya mencionada, no solicitada o que oculte total o parcialmente la identidad del remitente o sin una dirección de correo electrónico válida a la cual el usuario consumidor pueda enviar una petición o solicitud para que tales comunicaciones cesen, cometerán infracción a la presente ley, sin perjuicio de las acciones legales que se entreguen al usuario consumidor.

Si bien este proyecto, tampoco vio la luz[178], ya contenía ideas y conceptos que de una u otra manera fueron replanteadas al modificar la ley de Defensa de los Derechos de los Consumidores.

C.- Proyecto que origino la Ley Nº 19.955

Esta ley modifico la ley de Defensa de los Derechos de los Consumidores Nº 19.496, incorporando un atisbo de legislación antispam, cuya efectividad hasta el día de hoy ha sido casi nula.

El proyecto original, cuya iniciativa fue del Presidente **Ricardo Lagos Escobar**, no contemplaba ni en su mensaje, ni en texto mismo del proyecto las normas que finalmente vieron la luz respecto de las comunicaciones comerciales no solicitadas.

Estas surgieron de la discusión que realizo la C**omisión de Economía,**

178 Archivado el 19 de junio de 2003

Fomento y Desarrollo de la Cámara de Diputados[179], la cual luego de aprobar el proyecto en general y de aprobar en particular y sin debate los artículos propuestos por el ejecutivo y que no fueron objeto de modificaciones, generó un debate respecto de cada artículo que había sufrido modificaciones y que no existía unanimidad al interior de la comisión.

En efecto, la señalada comisión y a instancia de los Diputados señores Saffirio, Vargas, Correa y Uriarte, quienes formularon una indicación para sustituir el artículo 28-B del mensaje, por el siguiente:

"***Artículo 28-B.-Constituye infracción a lo dispuesto en esta ley el envío de comunicaciones publicitarias o comerciales por correo electrónico u otro medio de comunicación equivalente, incluyendo llamadas telefónicas automatizadas y faxes que no hubieran sido previamente solicitadas por el consumidor o expresamente autorizadas por éste.***
Cuando el consumidor solicite o autorice el envío de las comunicaciones comerciales o publicitarias por los medios señalados en el inciso anterior, el mensaje deberá ser claramente identificable como tal, debiendo individualizarse la persona en nombre de la cual se realiza y, la dirección de correo electrónico a la cual se puede solicitar la suspensión de tales comunicaciones. En cualquier momento podrá dejar sin efecto la autorización dada para el envío de dichas comunicaciones, situación en la cual el proveedor deberá eliminar los datos del consumidor y, en caso de haberlos comunicado a terceros, informarles de la revocación."

179 La comisión estaba integrada a la fecha de la votación por los Señores Diputados Francisco Encina; Carlos Hidalgo; Pablo Prieto; Fulvio Rossi; Eduardo Saffirio; Edmundo Salas; Eugenio Tuma; Gonzalo Uriarte y Patricio Walker.

En el Senado, en la Comisión de Economía[180], en sesiones celebradas el 10 y el 17 de junio de 2003, expresó en su primer informe, fechado el 30 de junio de 2003, que aprueba en general dicho proyecto, pero propuso al Senado que la iniciativa fuera examinada en el tramite reglamentario del segundo informe, por esta Comisión, en conjunto con la Comisión de Constitución, Legislación, Justicia y Reglamento Unidas.

En su segundo informe, de fecha 16 de marzo de 2004, la Comisión[181] respecto de esta norma formulo dos indicaciones, la 47 y la 48. La primera de ellas, de autoría de los Honorables Senadores señores Chadwick y Novoa, propuso sustituir el artículo 28 B por otro que indica que la remisión de publicidad a través de los medios señalados deberá indicar una dirección válida a la que el destinatario pueda solicitar la suspensión del envío de dichas comunicaciones. Además, estableció que debería solicitarse expresamente la autorización del destinatario para utilizar su dirección de correo electrónico con el objeto de enviarle comunicaciones, en caso de que el prestador la hubiera obtenido durante el proceso de compra de un bien o de contratación de un servicio.

Por su parte, la otra indicación, de autoría del Honorable Senador señor Viera-Gallo, incluye en el artículo 28 B una referencia al correo postal y a los servicios o llamados de mensajería telefónica.

La Comisión aprobó las indicaciones en análisis con modificaciones, refundiéndolas. Entre las menciones que deberá contener la comunicación, se agrega la materia o asunto sobre la que ella versa; se

180 La Comisión fue integrada por los Honorables Senadores Señores Jovino Novoa Vásquez; Jaime Gazmuri Mujica; José García Ruminot; Jorge Lavanderos Illanes y Jaime Orpiz Bouchon
181 Acordado en sesiones de fechas 9 y 16 de diciembre de 2003 y 13 de enero y 2 de marzo de 2004, con asistencia de los HH. Senadores señores Jovino Novoa Vásquez (Presidente), José García Ruminot, Jaime Gazmuri Mujica, Jorge Lavandero Illanes y Jaime Orpis Bouchon.

omite la referencia al correo electrónico, porque ese punto es regulado en otro precepto, y se alude, en cambio, al correo postal, el fax y los servicios telefónicos; se prohíbe, finalmente, remitir nuevas comunicaciones al consumidor que haya solicitado suspender el envío de las mismas.

El Honorable senador señor Novoa manifestó que la solución planteada en el proyecto aprobado con ocasión del primer trámite constitucional por la Cámara de Diputados, es extrema e impediría hacer publicidad por correo electrónico. La fórmula propuesta por la indicación aprobada, habilita a los destinatarios de la publicidad para exigir que se les excluya del envío de la misma.

Agregó que en los Estados Unidos de América se ha optado por una vía alternativa, cual es, establecer un registro de quienes no desean recibir publicidad por estos medios, lo que conlleva la necesidad de resolver problemas tales como quien debe tener a su cargo dicho registro o como se financian los costos que el mismo irrogue.

Ambas indicaciones fueron aprobadas con modificaciones, por la unanimidad de los miembros presentes de la Comisión, Honorables Senadores señores García, Lavandero, Novoa y Orpis, quedando el artículo propuesto de la siguiente manera:

Artículo 28 B.- Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos.
Los proveedores que dirijan comunicaciones promocionales o publicitarias a los consumidores por medio de correo postal, fax, llamados o servicios de mensajería telefónicos, deberán indicar una

forma expedita en que los destinatarios podrán solicitar la suspensión de las mismas. Solicitada ésta, el envío de nuevas comunicaciones quedará prohibido.".

Al respecto cuando se sometió a votación esta Ley en la Sala el Senado se solicito votación separada, pues según los dichos del Honorable Senador Novoa[182], ***"la propuesta de la Cámara de Diputados, contemplaba que para que una persona pudiera recibir una comunicación publicitaria por correo electrónico u otro medio equivalente, incluido el fax, tenía que autorizarla previamente. Quedaba prohibido, entonces, realizar publicidad a través de esos medios.***
Por ello la Comisión de Economía del Senado considero una solución distinta a la de la Cámara Baja, fundamentalmente porque era imposible regular desde Chile el principal problema, del spam, ni impedir a las casas comerciales, por ejemplo, que enviaran publicidad, pues sin duda, para mandar un correo electrónico desde el extranjero, nadie preguntaría antes cuál era nuestra legislación".

Continúo el Senador Novoa, "***que el spam, que es el correo que nos ahoga, no viene de fuentes conocidas. Entonces, en Chile, una ley que dijera "Se prohíbe esto" iba a afectar única y exclusivamente a las entidades establecidas aquí, que están obligadas al cumplimiento de la ley, y no corregiría el problema de la inundación de correo basura"***

La norma por ellos aprobada, permitía a su juicio una gran efectividad, ya que al establecerse que ***"Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la***

182 Diario de Sesiones del Senado. Legislatura 350. Extraordinaria. Sesión 53º. 4 de Mayo de 2004.

materia o asunto sobre el que versa," si a alguien no le interesa, lo elimine inmediatamente- "la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos.", de manera que "Pensamos en la Comisión que la forma de impedir el spam era establecer que el remitente del correo estuviera obligado a dar una dirección válida donde se le pudiera pedir que no siguiera enviándolo."

Agrego Novoa, que ***"Después de aprobada la norma, se nos señaló que tenía un problema, consistente en que, si uno contestaba un correo para solicitar que no se le enviara más, estaba validando una dirección, es decir, informando al remitente que ella era hábil y se encontraba en uso. Por lo tanto, permitíamos crear una base de datos mediante el envío de un correo a una dirección y la validación de ésta a través de la respuesta.***

Obviamente, era un punto por considerar y que, de alguna manera, posibilitaba revisar la conveniencia de una posición distinta. Y a eso obedece la indicación presentada ahora por el Ejecutivo, que no va al extremo de prohibir la publicidad, sino que establece un mecanismo en virtud del cual no es necesario contestar los correos para pedir que no se sigan enviando, ya que el silencio produce el mismo efecto.

Sé que este problema es bastante complejo, porque no resulta fácil decidir acerca de la solución más adecuada. Desde luego, no parece razonable prohibir que se remitan comunicaciones publicitarias o promocionales. La publicidad es un elemento importante del comercio. Y la publicidad barata -eventualmente, la realizada a través del correo electrónico, de Internet- puede permitir el desarrollo de pequeñas y medianas empresas, de innovadores, de personas que ofrecen prestación de servicios. Entonces, si

consagramos una prohibición al respecto, probablemente afectaremos a quienes no tengan capacidad económica para hacer publicidad a través de la radio, la televisión, los diarios.
Entonces, muchas veces, cuando se aprueban normas con muy buenos propósitos, como el de impedir que nos inundemos de correo basura, la prohibición puede provocar consecuencias negativas que -estoy seguro- el legislador no desea.
Por eso solicité votación separada de este artículo, con el objeto de que consideremos como alternativa la proposición del Ejecutivo".

Luego debidamente autorizado, intervino el señor Alberto Undurraga, Director Nacional del Servicio Nacional del Consumidor, quien señalo que ***"Es un hecho que los correos electrónicos publicitarios requieren algún tipo de regulación, no sólo por la molestia que genera el recibirlos, sino también porque involucran un conjunto de costos para la economía, para el proveedor de servicios de Internet y, naturalmente, para el consumidor.***
En el mundo entero se está enfrentando ese problema. Y hay sobre el particular dos soluciones que bien pueden reflejar los planteamientos de la Cámara de Diputados y de la Comisión de Economía del Senado.
En la Cámara Baja se aprobó el año pasado la prohibición expresa de tales correos, salvo que cada consumidor los acepte. Efectivamente, eso resuelve el problema, pero al costo de no permitir la publicidad barata a las empresas pequeñas y a las microempresas.
Ésa es la solución europea.
El Senado apunta más a la solución norteamericana: posibilitar el envío de un primer correo, pero permitiendo al consumidor rechazarlo a determinada dirección del remitente. En la práctica,

con esto se valida la dirección del destinatario -como mencionó el Senador señor Novoa- para el posterior comercio de bases de datos.
Por lo tanto, en la indicación que ingresó hoy -si es preciso, puede reconsiderarse su discusión- planteamos una solución intermedia: permitir a todas las empresas inscritas gratuitamente en un Registro administrado por la Subsecretaría de Economía enviar ese tipo de correos y que no puedan hacerlo aquellas que no estén registradas.
La indicación señala que, respecto de los correos enviados por una persona o empresa no registrada, el Servicio Nacional del Consumidor o el consumidor que los esté recibiendo podrá solicitar al proveedor de servicios de Internet que los filtre, que no los deje entrar. Eso, técnicamente, es posible.
Por lo tanto, de esa manera también se soluciona el problema de los spam provenientes del exterior."

Al respecto luego de un intenso debate, protagonizado principalmente por la Honorable Senadora Matthei, quien en definitiva votó en contra de la indicación, se aprobó la norma propuesta por la Comisión, desoyéndose la indicación de última hora del ejecutivo.

Devuelto el Proyecto en tercer Tramite Constitucional la Cámara de Diputados[183] aprobó tras un intenso debate la indicación tal cual había sido propuesta por la Comisión de Economía del Senado.

En consecuencia de lo anterior, hoy en Chile la Ley del Consumidor sanciona esta práctica comercial, pues considera que vulnera el derecho a la libre elección del consumidor, y su derecho a la privacidad. Por lo tanto, los usuarios tienen derecho a exigir que se les remueva de las listas de

183 Diario de Sesiones de la Cámara de Diputados. 350º Legislatura Extraordinaria. Sesión 84. 12 de Mayo de 2004.

destinatarios.

Por ello, la ley obliga a quien envíe una comunicación promocional o publicitaria por correo electrónico, a indicar:

(1) la materia de que se trata en el encabezado (asunto o subject).
(2) identificar quién envía el correo (remitente)
(3) indicar una dirección válida a la que se pueda solicitar la suspensión de los envíos.

La individualización de quién envía el correo debe permitir saber qué proveedor está detrás, su nombre, domicilio, actividad, representantes, teléfonos y todo otro dato relevante. Los correos anónimos o con información incompleta infringen la Ley.

Si una vez solicitada la suspensión de los mensajes, el envío persiste, el remitente podrá ser castigado con una multa de hasta 50 UTM (un millón y medio de pesos aproximadamente).

D.- Proyecto Jovino Novoa

Proyecto de Ley, que busca modificar la ley nº 19.628 en lo que se refiere a la publicación de boletines con información de datos personales-patrimoniales, con el objeto de proteger más adecuadamente los derechos de las personas y de las pymes. Además, propone modificar la ley para dar una mejor protección a los "datos sensibles" y hacerse cargo de los problemas derivados del "Spam"[184]. Dicha moción fue presentada con

[184] BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº **3796-07** . [en línea] Chile. [Fecha de consulta: 30 abril 2007] Actualización permanente. Disponible en: http://www.bcn.cl/

fecha 1 de marzo del presente año por el Senador Jovino Novoa a la Comisión de Constitución de la cámara alta, y con fecha 15 de marzo de 2005 por Oficio Nº368-352 de S.E el Presidente de la República mediante el cual incluye esta iniciativa en la nómina de proyectos que podrán ser tratados en la Legislatura Extraordinaria Nº 352, y en este momento se encuentra en primer tramite constitucional.

Básicamente y a modo de introducción este proyecto aborda dos situaciones entrelazadas, como solución a la problemática del Spam. La primera pretende mediante la conversión de la dirección de Correo electrónico en un dato de carácter sensible; y en segundo lugar intenta regular el Spam como tal.

En primer lugar para adentrarnos adecuadamente en este tema es importante definir algunos conceptos previos, de manera de que podamos esclarecer claramente los que es un Dato Sensible.

Podemos decir que el ser humano, para representar lo que le interesa transmitir en un mensaje, utiliza un código común preestablecido entre el emisor y el receptor del mismo, y que generalmente lo podemos englobar en la palabra, tanto en forma escrita como oral.

En tal sentido, el DATO "***es una representación de una porción de la realidad expresada en términos que forman parte de un código preestablecido de manera que pueda ser interpretado, y que está destinado a dar esa información a un receptor***", de allí su origen etimológico, la palabra, "datum", que en latín significa "dado", participio del verbo "dar"[185].

185 GHIGLIANI, Leonardo. Datos Personales: Propiedad Y Derecho Al Uso. Estudios sobre Tecnología y Privacidad - Datos personales - Habeas Data.

Esta comunicación puede concretarse por ejemplo en una conversación, en un aviso publicitario, puede representarse en un objeto para ser descifrado más adelante, tal como sería el caso de un libro, un archivo,etc, Según el profesor **Miguel S. Elias,** citando a Molina Quiroga, el dato es una "***mínima unidad de información***"[186], que puede consistir ya sea en un punto, una frase, un número, una cifra, un articulo de un código, una nota musical, una imagen, etc.

En virtud de lo anterior, podemos observar que el "dato" no se limita únicamente al texto, ya que perfectamente puede ser una foto, que es información, y que al descomponerla en diversas partes, haga de cada una un dato independiente, o sea, una "mínima unidad de información" independiente.

En otro orden de ideas debemos señalar que un Banco de datos son un conjunto de datos e informaciones recogidas, acumuladas y clasificadas por cualquier medio, tal como sería la que contiene los nombres de los clientes de una empresa, la que mantiene Dicom para información financiera, la que manejan las policías respecto de delincuentes, etc.

Como se puede observar, se trata simplemente de una pluralidad de datos agrupados en un mismo conjunto, que pueden estar en diversos formatos, como son el cada vez menos tradicional soporte en papel impreso (por ejemplo el Registro de Propiedades del Conservador de Bienes Raíces y sus añosos libros, o en un soporte digitalizado o electrónico.

Capítulo 2[en línea] Argentina. [Fecha de consulta: 1 mayo 2007] Disponible en: http://www.it-cenit.org.ar/Publicac/PeopleBases/Recopilac/Recopilac2.htm#que%20son%20los%20datos

186 Miguel S. Elias. Situación legal de los datos de carácter personal frente a las nuevas tecnologías.Biblioteca Eletrônica. Régimen Jurídico de los Bancos de Datos . [en línea] Argentina. [Fecha de consulta: 1 de mayo de 2007] Disponible en: http://www.aaba.org.ar/bi130014.htm.

Sin duda, el impacto y el incontenible avance de la nuevas tecnologías en la vida cotidiana de todos los ciudadanos "la Revolución Tecnológica", genera la necesidad de proteger cada vez más la intimidad y privacidad frente a una innumerable cantidad de violaciones a dichos derechos que se producen por la falta de una protección legal clara y precisa.

Este fenómeno reciente es el que se denomina como la "***Sociedad del Conocimiento o de la Información***", producido en gran parte por esta revolución digital o tecnológica en la que estamos inmersos, siendo uno de los máximos exponentes la red Internet.

Volviendo a la idea de Dato, debemos preocuparnos por señalar que es un DATO PERSONAL, los cuales "son aquellos que tienen características identificatorias de las personas o que se les pueden imputar a ellas; adquiriendo una vital importancia temas como la regulación de su uso, su manipulación y su protección legal."[187]

La antigua ley española de protección de datos personales (L.O.R.T.A.D.)[188] los define como "cualquier información concerniente a personas físicas identificadas o identificables", idea que siguió el legislador nacional en la ley 19.628, y que ahora se piensa modificar al incorporar a las personas jurídicas.

Demás esta decir que estos registros personales no son nuevos, han existido desde que el hombre pudo exteriorizar sus ideas en forma escrita, realizándose toda clase de registros individuales en diversos formatos que

187 Miguel S. Elias. Situación legal de los datos de carácter personal frente a las nuevas tecnologías.Biblioteca Eletrônica. Régimen Jurídico de los Bancos de Datos . [en línea] Argentina. [Fecha de consulta: 1 de mayo de 2007] Disponible en: http://www.aaba.org.ar/bi130014.htm.

188 La "Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal" (LORTAD), Nº 5/92, de España fue sancionada el 29 de octubre de 1992. Fue modificada por la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD), pero manteniendo el mismo concepto.

se caracterizaban por necesitar grandes espacios físicos que permitieran su correcta administración, almacenamiento, recuperación y control.

Hoy la realidad es otra ya que se nos presenta un nuevo problema, ya que las nuevas tecnologías han entrado en nuestras vidas.

Con la digitalización de esos viejos registros y ficheros se ha logrado que cobren un impensado valor comercial, estadístico, jurídico y social, adquiriendo una relevancia sumamente trascendente, logrando, además, un enorme abaratamiento de los sistemas de almacenamiento.

Esto se da, en gran parte, en función de la posibilidad de entrecruzarlos y combinarlos entre sí, permitiendo un ensamble con otros datos; de recuperar rápidamente los mismos, accediendo a ellos en forma totalmente automatizada; y de que estas bases automatizadas se generen y vinculen por sí solas.

Contra este fenómeno se ha acudido a la defensa de los derechos establecidos en las Constituciones Nacionales de los diferentes países, particularmente a la defensa del derecho a la intimidad y a la privacidad.

Tanto los Estados Unidos como la Unión Europea han sido los principales promotores del análisis del tratamiento de los datos personales para reforzar la posición de los ciudadanos frente a la rapidez, facilidad e incontrolada utilización de datos que pudiera, de una forma u otra, generar un perjuicio a las personas.

En nuestro país, el art. 19 Nº 4 de nuestra Constitución Política consagra "El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia", en el Nº 5 establece "La inviolabilidad del hogar y

de toda forma de comunicación privada", garantizándose así, el ámbito de privacidad de las personas; el cual obviamente debe alcanzar la esfera de la tecnología y las aplicaciones que por tales se está realizando en el mundo entero.

Por ello es de suma importancia determinar, tanto los datos a utilizar, como la forma de su tratamiento y cual es el fin que ellos tendrán, lo que de una u otra manera permitirán dar el carácter de mayor o menor protección a ellos, ya que no debemos dejar de lado que el desarrollo de las bases de datos personales produce resultados altamente positivos acarreando enormes ventajas tanto en las ramas científica, comercial y de políticas públicas, como es en materia de salud, de educación y de seguridad, a través de la realización de informes y estadísticas. Es decir, que estamos frente a algo positivo que, para que no produzca resultados no deseados, debe ser estudiado a fondo y regulado correctamente. Por ejemplo, el Profesor Elías, citando un artículo de David Casacuberta, denominado "listas Negras en la Red", en los EE.UU. en materia de salud[189] se está trabajando en un sistema nacional que contendrá las historias clínicas de todos los habitantes, lo que permitirá no sólo proporcionar ayuda instantánea en caso de una urgencia en cualquier lugar del país (y aun del exterior) sino además prevenir epidemias, tener información en tiempo real sobre el estado de salud de la población. El concepto de la "transparencia" recurrentemente utilizado por los economistas para calificar a los mercados, es perfectamente adaptable. En los EE.UU. un sitio proporciona información sobre sueldos, que es especialmente útil tanto para las búsquedas laborales como para hacer estudios.

189 Miguel S. Elias. Situación legal de los datos de carácter personal frente a las nuevas tecnologías.Biblioteca Eletrônica. Régimen Jurídico de los Bancos de Datos . [en línea] Argentina. [Fecha de consulta: 1 de mayo de 2007] Disponible en: http://www.aaba.org.ar/bi130014.htm

Hechas las aclaraciones anteriores, podemos señalar siguiendo al profesor Miguel Elias[190], que los datos personales se podrían clasificar en dos ramas específicas: los datos personales íntimos (subdivididos, a su vez, en datos "sensibles" y "no sensibles" y los datos personales públicos.

Los "Datos personales íntimos" según gran parte de la doctrina se dividen en datos "sensibles" y "no sensibles".

Los **DATOS PERSONALES "SENSIBLES",** los podemos definir como aquellos que por sí solos impulsan naturalmente a un individuo a la más íntima y absoluta reserva de dicha información.

Obviamente y en atención a su carácter, requieren una regulación sumamente fina, detallada y muy especial que proteja correctamente la difusión de este tipo de datos; como pueden ser aquellos relativos a la salud, (padecimiento de enfermedad de transmisión sexual), a la identidad o vida sexual, a ciertos tipos de ideologías o creencias, o a cualquier clase de información que implique un carácter de absoluta reserva para el individuo, por pertenecer a su esfera de intimidad y conciencia y que su divulgación lo coloque en una situación de extremada incomodidad social.
Sabido es que una de las facetas de la libertad de intimidad es el derecho al secreto. Este consiste en la simple facultad de reservarse ideas, sentimientos, conocimientos y acciones que el sujeto no desea dar a conocer voluntariamente; reuniendo los caracteres propios de los derechos personalísimos: innato, necesario, esencial, privado, inherente, vitalicio, de objeto interior, relativamente disponible y autónomo.

190 Miguel S. Elias. Situación legal de los datos de carácter personal frente a las nuevas tecnologías.Biblioteca Eletrônica. Régimen Jurídico de los Bancos de Datos . [en línea] Argentina. [Fecha de consulta: 1 de mayo de 2007] Disponible en: http://www.aaba.org.ar/bi130014.htm

El profesor **Horacio Lynch** plantea el interrogante y pone en duda esta clásica distinción de datos personales "sensibles" y "no sensibles" diciendo que carecen de sentido ya que perdieron actualidad.[191] En efecto, dicho autor plantea que lo que ahora determina la sensibilidad es la forma en que se manipulan esos datos, ya que la sumatoria de datos "no sensibles" produciría información "sensible". A igual conclusión se llego en un fallo del Tribunal Constitucional Federal Alemán en un fallo de 1983, con ocasión de la promulgación de la ley del Censo, al señalar con relación al "Derecho a la autodeterminación informativa" que "Lo único que procede decidir es el alcance de este derecho en cuanto a las injerencias en las cuales el Estado exige al ciudadano la comunicación de datos relativos a su persona, y en este punto no es posible tomar como referencia única la clase de datos. Lo decisivo es la utilidad y la posibilidad de utilización de los mismos, los cuales dependen, por una parte, de la finalidad a la que sirve la encuesta y, por otra, de las posibilidades de la oración e interrelación propias de la tecnología informativa que se emplee. De este modo, un dato carente en sí mismo de interés puede cobrar un nuevo valor de referencia, y en esta medida ya no existe, bajo las condiciones de la elaboración automática de datos, ningún dato "sin Interés" / A consecuencia de lo que antecede, el grado de sensibilidad de las informaciones ya no depende únicamente de si afectan o no a procesos de la intimidad. Hace falta más bien conocer la relación de utilización de un dato para poder determinar sus implicancias para el derecho de la personalidad. Sólo cuando reine la claridad sobre la finalidad con la cual se reclamen los datos y que posibilidades de interconexión y de utilización existen se podrá contestar la interrogante sobre la licitud de las restricciones del derecho a la autodeterminación informativa."[192]

En el fondo, interpretando el dato sensible en sentido estricto como aquel

---

191 Lynch, Horacio. Notas sobre el Derecho en la Era Digital. Biblioteca Electrónica. Régimen Jurídico de los Bancos de Datos. [en línea] Argentina. [Fecha de consulta: 1 de mayo de 2007] Disponible en: http://www.it-cenit.org.ar/Publicac/DERDIG.

192 Tribunal Constitucional Alemán. Sentencia 15 de Diciembre de 1983. Ley del Censo (Volkszählungsgestz 1983)

que por si sólo genera una esfera proteccional por parte del individuo, no se aparta de la sensibilidad que podría producir una acumulación de datos no sensibles.

En cuanto a los **DATOS PERSONALES "NO SENSIBLES",** podemos señalar que son aquellos que se refieren a un sujeto individualizado y son relativos a su fuero interno o íntimo sin llegar a ser información puramente sensible. Identifican su personalidad, sus creencias e ideologías, sus pensamientos, sentimientos y salud, entre otras cosas.

En definitiva, son los relacionados al orden privado de los individuos que los hacen merecedores de una protección más profundizada y específica que los demás tipos de datos generales, debido a que se revelan exclusivamente de forma particular e individual, y rara vez son objeto de tratamiento público.

Su problemática radica en que desagregando estos datos íntimos de las diversas bases de datos existentes de una misma persona, y asociándolos entre sí, se podrían llegar a crear perfiles de la personalidad que muchas veces podrían llegar a ser arbitrarios o inexactos. Precisamente esto es lo que Lynch sostenía al decir que realizando un tratamiento especial sobre datos no sensibles, se creaba información sensible.

Esta clase de datos personalísimos pertenecen, en principio, a la persona física que los genere, detente y, por ende, pueda disponer de ellos.

Por ello, por la naturaleza misma que poseen y salvo que mediara un consentimiento expreso del individuo al que el dato de carácter personal hace referencia, no deben ser objeto de manipulación, tratamiento o divulgación de ningún tipo.

Hay que considerar también como excepción cuando una limitación de acceso a los mismos pueda afectar directa o indirectamente cuestiones relacionadas a la seguridad, a la defensa del Estado o Políticas Públicas.

En estos casos concretos, por una disposición especial expresa y a ese sólo efecto, se podría acceder a esta información reservada, en principio, a la esfera íntima del ser. Pero de este tema hablaremos posteriormente.

En cuanto a los Datos personales públicos, podemos señalar que son aquellos datos que constan en numerosos registros de carácter público o privado.

A modo ejemplar serían el nombre y apellido, domicilio, estado civil, filiación, número de teléfono, números identificatorios como el Rol único Tributario o la Cédula de Identidad y el pasaporte, título profesional, seguros y créditos obtenidos y el patrimonio, entre otras muchas variantes. Como se puede ver se trata de referencias que permiten identificar o situar a las personas individuales y su entorno cotidiano y, por lo tanto, caen en el ámbito personal de las mismas.

Los registros públicos son aquellos que obran en organismos del Estado, e incluso los que tienen carácter secreto. Algunos de ellos son los Registros del INE, el Registro Electoral, El Registro Civil de Identificación, etc. Por otra parte existen Registros privados, que se ponen a disposición del público, como ocurre con las Bases de Datos de Dicom.

Este tipo de datos muchas veces suelen ubicarse tanto en la categoría de datos privados como de datos públicos. Si bien se refieren a una persona determinada, comprenden a su vez, aspectos públicos de la personalidad del individuo (apellido, nombres, estado civil, estudios cursados, labores

que desempeña, etc.). Es decir, pueden tener trascendencia para la esfera íntima de la persona (por ejemplo, el nombre, que es íntimo de las personas) pero también en la esfera pública de la misma (usando el mismo ejemplo, el nombre de las personas se encuentra inscripto en el Registro Civil).

La consideración del dato como perteneciente a una u otra clase es subjetiva aunque, a efectos de establecer protecciones legales de dichos datos, es necesario establecer definiciones y reglamentaciones en cuanto a su tratamiento, ya sea manual o automatizado.
Hechas las aclaraciones, respecto al dato, su caracterización como personal o público, sensible o no, corresponde analizar la situación especial del Dato sensible.

Tal como se señaló anteriormente, aquellos que por sí solos impulsan naturalmente a un individuo a la más íntima y absoluta reserva de dicha información, de manera que su divulgación lo coloque en una situación de extremada incomodidad social.

En atención a lo anterior, cuando el Nº 7 del proyecto propone incorporar a través del artículo 10 A, a "El dato personal dirección de correo electrónico poseerá la calidad de sensible…", es importante señalar que la legislación comparada, no le da el carácter de sensible a las direcciones de correo electrónico, toda vez que el objeto apunta precisamente a proteger datos que de una u otra manera puedan afectar a la persona al invadir su privacidad, como ocurre si se publicaran aquellos datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

En tal sentido, no se encuentra ninguna razón para que se le incorpore a especial protección, toda vez que por mucho que se conozca la dirección electrónica de alguien, ello no significa que se tenga acceso a información que ponga en peligro la integridad de los mismos. Si no que queda de manifiesto que su carácter de dato sensible, es exclusivamente para intentar detener el Spam y sus consecuencias económicas, que afectan tanto a la industria como a los usuarios de correo.

No obstante lo anterior, debemos mencionar que algunos autores estiman, tal como **Alejandra Castro Bonilla**, Profesora Costarricense[193], "que el correo electrónico es un conjunto de datos personales del usuario y como tal, y su manipulación se encuentra supeditada a las normas relativas a la protección de datos personales. / Con los datos obtenidos a través de una cuenta de correo EVENTUALMENTE se puede constituir el perfil de un usuario, quedando vulnerada con ello su intimidad, su vida privada. Por ejemplo, a simple vista una dirección puede evidenciar el nombre y apellidos del usuario, el lugar geográfico de origen, su lugar de trabajo e incluso aspectos más delicados como su inclinación política, religiosa o sexual, dependiendo del servidor que proporcione la dirección de correo o el nombre de dominio. En el caso que el usuario haya proporcionado más datos de su vida privada en el momento de adquirir la cuenta, también desde su perfil se pueden determinar números de teléfono, dirección domiciliaria, gustos o incluso su profesión. Dentro del conjunto de datos también la transmisión de mensajes electrónicos hace posible que pueda averiguarse la dirección IP del usuario que es en sí misma un dato personal, pues si se llega a descifrar la misma, se puede identificar la terminal del usuario (y en ocasiones con cierta destreza acceder a sus archivos) pero también la situación nominativa del titular. Todo esto pone

193 BONILLA Castro, Alejandra "El uso legítimo del correo electrónico" Delitos Informaticos.com [en línea] [Fecha de consulta: 1 de mayo de 2007] Disponible en: http://delitosinformaticos.com/delitos/correo4.shtml

en evidencia que el correo electrónico condensa una serie de datos del individuo, cuya manipulación (muchas veces invisible para el usuario) podría poner en vulnerabilidad su derecho a la autodeterminación informativa."

Pese a lo señalado anteriormente, y teniendo claro que una mano experta en internet, podría llegar a obtener toda esa información a través de una dirección de correo electrónico, la normalidad de las personas no tiene dicha opción, razón por la cual no se encuentra la justificación para darle dicha protección, calificándola de "información personal de carácter sensible", aun cuando muchos expertos latinoamericanos así lo quieran.
Además, hay que considerar lo expresado por la doctrina y jurisprudencia extranjera ya citada, que lo que a la larga dará la sensibilidad de un dato, será el tratamiento que se da los datos y la cruza que se haga de las distintas bases de datos, con lo cual hasta el dato mas insignificante podría llegar a convertirse en un Dato Sensible.

Tal como señalamos es el apropiado tratamiento de los datos, el que permite convertirlos en información útil para el logro de determinados objetivos. Pero esos datos, obviamente, pueden amenazar la dignidad de los hombres por el uso arbitrario y malicioso de la informática.

Esta necesaria protección es un límite al manejo de la informática ante el temor de que pueda atentar la intimidad de los ciudadanos y que pueda restringir el ejercicio de sus derechos.

Sabemos que una base de datos, esta compuesta por todo tipo de información aportados por las personas para determinados fines. Pero también existe una gran variedad de medios a través de los cuales se compila información de las personas sin su consentimiento, tal como

sucede en algunos sitios de Internet que cruzan datos de las personas que las visitan y conforman un perfil del interesado.

La existencia de enormes bases de datos que contienen gran cantidad de información referida a las personas, es una consecuencia de la informática y sin la cual seria imposible su existencia.

Lo importante es la finalidad para el cual se usará la información allí almacenada para evitar que seamos discriminados debido a un uso desatinado de sus datos.

La cuestión es aun más grave si especulamos que esas bases de datos pueden ser atacadas por crackers que son aquellos aficionados a la computación que obtienen accesos no autorizados a los sistemas informáticos, robando o destruyendo datos, y que buscan información para si o para terceros.

La ambición para conseguir datos no es el mismo que para actualizarlos, rectificarlos, suprimirlos o modificarlos.

La doctrina especialista en el tema, se refiere al amparo debido a los ciudadanos contra la posible utilización por terceros de sus datos personales susceptibles de tratamiento automatizado para confeccionar una información que afecte a su entorno personal, social o profesional en los límites de su intimidad.

La protección de datos está prevista por las innovadoras legislaciones mediante el derecho a la intimidad y su transmisión telemática cuando aparece una nueva relación entre datos y personas que necesitan ser protegidos mas allá de las normas referentes a la intimidad.

Lo primordial es que los datos no generen situaciones de segregación o discriminación por cuestiones de salud, raza, ideas, costumbres y datos que pudieran llegar a limitar nuestras posibilidades.

Tal como señalamos anteriormente, son bases de datos privadas los datos que tienen regulados situaciones o circunstancias en que la persona se ve obligada a darlos o ponerlos en conocimiento de un tercero, debiendo impedir su difusión y respetar la voluntad de secreto sobre ellos, de su titular. A su vez, dentro de los privados encontramos los datos personales íntimos, que son aquellos que el individuo puede proteger su difusión frente a cualquiera y que, de acuerdo con un fin determinado, esta obligado a dar, salvo algunas excepciones.

Estos datos forman parte de aquellos que se encuentran debidamente resguardados por nuestra Constitución Política del Estado, en el art. 19 Nº 4. al señalar "Art. 19. La Constitución asegura a todas las personas: 4º.-El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia".

De igual modo, tienen derecho a conocer a actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Y como datos personales que requieren una protección especial, tales como ideas políticas, creencias religiosas, salud física o mental, comportamiento sexual de los individuos y la autodeterminación informática.

Este es el derecho conocido como habeas data, considerado hoy como uno de los más importantes derechos fundamentales, especialmente dado el desarrollo de la cibernética, la informática y la telemática y en general de la información y las comunicaciones en la actualidad"

Para una mayor ilustración analizaremos el término de Intimidad: según el **Diccionario Jurídico Espasa**[194] "***es un derecho constitucionalmente reconocido y protegido, es objeto de tutela en la diversas ramas del ordenamiento jurídico, entre ellas la penal", según el Diccionario de la Academia de la Lengua Española, es la zona espiritual y reservada de un grupo de personas; esta definición coincide con la llamada "doctrina de la autodeterminación informativa***", creada por el Tribunal Constitucional Alemán en un fallo del 15 de diciembre de 1983, donde se instituye que es titular de los datos personales la propia persona y debe ser requerido su consentimiento por parte de terceros que deseen almacenarlos, cederlos o publicarlos; el Diccionario Jurídico de Ossorio y Gallardo, define al derecho a la intimidad como "el derecho que tienen las personas a que su vida intima sea respetada, que nadie se entrometa en la existencia ajena publicando retratos, divulgando secretos, difundiendo correspondencia, mortificando a otros en sus costumbres y perturbando de cualquier otros en sus costumbres y perturbando de cualquier otro modo su intimidad."

Por su parte, la **Corte Constitucional de Colombia**, ha señalado que el derecho de la intimidad: "***Es un derecho entonces, personalísimo, según inspiración constitucional relativa a la dignidad humana, que debe ser tutelado cuando, por la acción de terceros, se produce una intromisión indebida en el ámbito personal o familiar del sujeto que conlleva la revelación de asuntos privados, el empleo de su imagen o de su nombre, o la perturbación de sus afectos o asuntos más particulares e íntimos relativos a su sexualidad o salud, con o sin***

194 Diccionario Jurídico ESPASA. Espasa Siglo XXI. Edi.1998. Pág. 534

divulgación en los medios de comunicación.[195]"

Se ha considerado doctrinariamente, que constituyen aspectos de la órbita privada, los asuntos circunscritos a las relaciones familiares de la persona, sus costumbres y prácticas sexuales, su salud, su domicilio, sus comunicaciones personales, los espacios limitados y legales para la utilización de datos a nivel informático, las creencias religiosas, los secretos profesionales y en general todo "comportamiento del sujeto que no es conocido por los extraños y que de ser conocido originaría críticas o desmejoraría la apreciación" que éstos tienen de aquel.[196]

El avance de este derecho en caso alguno es reciente, ya que podemos remontarnos al año 1890 donde una publicación en el diario "Harward Law Review" salvaguardaba la propiedad de cada individuo sobre la propia privacidad, como el derecho de estar sólo (to be let alone); pero en el siglo XX, el derecho a la intimidad adquiere un predominio especial ya que actualmente cubre un cúmulo de relaciones que el individuo mantiene sobre otros y que deben ser preservados como de su reserva personal.

El derecho a la intimidad es el derecho de toda persona a que se le respete en su vida privada y familiar, y a evitar injerencias arbitrarias en la zona espiritual íntima y reservada de una persona.

El llamada "nuevo derecho a la intimidad" posee una faz preventiva y una faz reparadora: preventiva por la facultad de conocer los datos personales que constan en registros automatizados, de exigir la rectificación,

195 Sentencia SU 089 de 1995 del Dr. Jorge Arango Mejía. Sentencia citada por la Corte Constitucional en la T-411 de 13 de Septiembre de 1995. MP. Alejandro Martínez Caballero. 13 de Septiembre de 1995 S. U - 089 de 1995. Disponible en: http://www.diritto.it/sentenze/straniere/sent_colombia.pdf. [Fecha consulta: 3 de Mayo de 2007]
196 Sentencia SU 089 de 1995 del Dr. Jorge Arango Mejía. Sentencia citada por la Corte Constitucional en la T-411 de 13 de Septiembre de 1995. MP. Alejandro Martínez Caballero. 13 de Septiembre de 1995 S. U - 089 de 1995. Disponible en: http://www.diritto.it/sentenze/straniere/sent_colombia.pdf. [Fecha consulta: 3 de Mayo de 2007]

actualización y cancelación de la información; y reparadora por al posibilidad de resarcimiento de daños y perjuicios por parte de quien lo padece.

En nuestro derecho positivo, que posee un rango constitucional, la evolución de este derecho puede resumirse desde el "secreto" al "control" de la información que se tiene de uno mismo en los bancos de datos.
Este derecho a la intimidad se encuentra por estos días seriamente amenazado por la capacidad que posee tanto el sector público como el privado, de acumular gran cantidad de información sobre los individuos en forma digital.

Con el desarrollo constante e ininterrumpido de la informática y las telecomunicaciones, se permite a tales entidades a manipular, alterar e intercambiar datos personales a gran velocidad y bajo costo. Así obtenemos sociedades altamente informatizadas en la que nuestras conductas y acciones son observadas y registradas y será imposible evitar la estigmatización y encasillamiento.

No se trata aquí de agotar el problema de la definición, sino nada más de dar noticias sobre las dificultades que existen al momento de determinar los elementos que la componen. Como no es difícil advertirlo, estas dificultades son uno de los escollos que deben ser superados al momento de legislar sobre el tema o aplicar la legislación vigente.

Los riesgos a los cuáles esta expuesta la vida privada de las personas en la sociedad de la información, en particular, aquellos derivados del tratamiento de datos personales a consecuencia de la utilización de las nuevas tecnologías de la información y de la comunicación, nos hacen cuestionar cual debe ser el rol del derecho ante la referida problemática.

En relación con el derecho a la intimidad, este hace referencia al ámbito personalísimo de cada individuo o familia, es decir, a aquellos fenómenos, comportamientos, datos y situaciones que normalmente están sustraídos a la injerencia o al conocimiento de extraños. Lo íntimo, lo realmente privado y personalísimo de las personas es, como lo ha señalado en múltiples oportunidades la Corte, un derecho fundamental del ser humano, y debe mantener esa condición, es decir, pertenecer a una esfera o a un ámbito reservado, no conocido, no sabido, no promulgado, a menos que los hechos o circunstancias relevantes concernientes a dicha intimidad sean conocidos por terceros por voluntad del titular del derecho a por que han trascendido al dominio de la opinión pública.

El derecho a la información expresa la propensión innata del hombre hacia el conocimiento de los seres humanos con los cuales se interrelaciona y de su entorno físico, social, cultural y económico, lo cual le permite reflexionar, razonar sobre la realidad, adquirir experiencias, e incluso transmitir a terceros la información y el conocimiento recibidos.

La Libertad Informática, como se le llama en España o Autodeterminación Informativa (nombre dado en España y Alemania respectivamente) ha sido denominada por la doctrina española y Alemana como "un nuevo derecho fundamental que tiene por objeto garantizar la facultad de las personas, para conocer y acceder a las informaciones que les conciernen, archivadas en bancos de datos y controlar su calidad, lo que implica la posibilidad de corregir o cancelar datos indebidamente procesados y disponer sobre su transmisión". Esta facultad, es lo que se conoce como Habeas Data que constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona en la esfera informática.

La Libertad Informática forma parte del núcleo de derechos denominados

de tercera generación, debido a que el derecho a la intimidad adquiere una nueva dimensión al verse amenazado por el uso abusivo de la informática. El mismo, bajo la forma de libertad informática, aúna la noción clásica de los derechos de primera generación, la libertad, en cuanto define las posibilidades reales de autonomía y de participación en la sociedad contemporánea, que pueden verse amenazadas por el mal uso que se haga de determinados datos personales; la igualdad, valor guía de los derechos de segunda generación, en cuanto en informática se concibe como un instrumento de control que puede introducir asimetrías entre quien controla ese poder y quienes no tiene acceso a él.

A éstos dos valores han de sumársele al hablar de derechos de tercera generación, el de la solidaridad ya que éstos derechos tienen una incidencia universal en la vida de los hombres, y con ella se apunta a garantizar su pleno disfrute, mediante un esfuerzo no egoísta de toda la comunidad.

El problema que se plantea en este escenario, y en especial sobre el control preventivo y el reparativo, que en Chile la señalada ley de datos adolece de una falta inexplicable y que no se compadece con la doctrina internacional, que casi en todo el resto de la ley se hizo, cual es, el no contar con una autoridad superintendente, que pueda realizar la revisión, el apoyo al afectado, de que los datos que se tienen de su propiedad sean o actualizados, bloqueados, removidos, etc.

El proyecto de ley que nos ocupa, bajo el epígrafe 4 de su mensaje, denominado "El problema de fondo y el contexto de la moción. La **"DIRECCIÓN DE CORREO ELECTRÓNICO"** como un dato personal y sensible, que debe protegerse en la ley n°19.628.", hace las siguientes consideraciones, que, no necesariamente llevan a concluir la caracterización de dato personal sensible de la dirección de Correo

electrónico.

Señala el mensaje del proyecto, y siguiendo al autor Renato Jijena; "que el abuso de las posibilidades computacionales constituye la amenaza por excelencia contra la intimidad, porque detentándose un enorme cúmulo de datos y cruzándose telemáticamente datos personales o nominativos, puede obtenerse un perfil determinado de las personas cuyos antecedentes son procesados. Esta imagen inmaterial debe ser resguardada porque puede ser creada errada o dolosamente, lo que eventualmente se traducirá en discriminaciones, en la imposibilidad de ejercer algún derecho, o en la pérdida de algún beneficio[197]".

Lo anterior lleva buscar la compatibilidad entre dos garantías constitucionales, por un lado el derecho a la intimidad, tanto en cuanto datos personales o nominativos, sensibles o no, procesados computacionalmente, y por otro el derecho a la información que reclama la sociedad toda.

El mencionado mensaje atiende a la contraposición de intereses legítimos de los titulares que han entregado sus datos y el uso que puedan darles organismos tanto de Gobierno o privados, para darles un uso legitimo a los mismos.

En dicho escenario el legislador ha llegado a la conclusión que para conciliar dichos intereses tan contrapuestos, de manera que se equilibre por un lado la máxima libertad o acceso a la información con un adecuado resguardo de la privacidad, hay que acudir a una respuesta doctrinaria, la cual ha entender "ha sido la formulación de un nuevo concepto del

197 JIJENA LEIVA, Renato; "Chile, la protección penal de la intimidad y el delito informático", páginas 9 y ss, publicado por la Editorial Jurídica Andrés Bello

Derecho a la Intimidad, que surge frente a la llamada o reclamada Libertad Informática o de procesamiento de datos personales-nominativos; que deja de lado el enfoque individualista o negativo con que fue concebido para plantearse desde una perspectiva socializadora y positiva (ya no es "el derecho a ser dejado a solas"); y que se concibe como la posibilidad de que los ciudadanos titulares y propietarios de los datos que les conciernan controlen el uso y el eventual abuso de los antecedentes que a su respecto sean recopilados, procesados, almacenados y cruzados computacional y telemáticamente".

Agrega que frente a ello se ha recurrido a la promulgación de las llamadas leyes de protección de datos, y Chile no ha estado ajeno a ese proceso.

En dicho escenario el legislador hace presente que la Ley chilena N°19.628 establece que en esencia, existen "datos personales" o nominativos que le pertenecen a sus titulares y que son "tratados" manual o automatizadamente, tanto por órganos públicos como por empresas o personas particulares, a quienes la ley califica como "responsables del registro o banco de datos".

Agrega que pese a constituir lo anterior la "regla general formalmente declarada por el texto legal" es que dicho "tratamiento de datos personales" sólo puede hacerse en virtud de autorización legal o del titular de los datos, pero del contexto de las normas se desprende que la mayoría de los datos provienen de "fuentes de acceso público" (por lo cual no se requiere de autorización para su tratamiento) y se consagran -como veremos- importantes y amplias excepciones sobre todo en materia de datos "personales-patrimoniales", lo cual transforma a la regla general en una mera declaración de principios.

Señala además, que "El mecanismo de resguardo recogido parcialmente

del Derecho Comparado se denomina "Derecho de Acceso" o "Habeas Data", y éste, después de ejercerse ante quien aparezca como responsable del banco de datos -si es que se tiene la suerte de ubicársele porque generalmente actúan en el anonimato- sólo puede reclamarse ante los tribunales ordinarios de justicia y no ante una autoridad administrativa".
En dicho orden de ideas, el mensaje señala que la moción parlamentaria en estudio, se basa "en propuestas presentadas en Congresos Internacionales por académicos y especialistas chilenos, que buscan soluciones definitivas y de fondo al problema. La principal de estas propuestas parte por entender que el tráfico previo y no autorizado de enormes listas y bases de datos con direcciones de correos electrónicos es un elemento que debe acotarse, porque se encuentra a la raíz del problema".

En tal orden de cosas, el legislador "Concibe luego a la dirección de correo electrónico de cada persona natural o jurídica como uno de sus datos personales y sensibles que le pertenecen y lo individualizan en la sociedad -es un atributo de su personalidad-, y por ende debe poder ser autodeterminado y controlado por sus titulares." Ello por cuanto estima que hay una desigualdad entre las personas "de los titulares de los datos personales que aspiran a controlar y autodeterminar el uso con fines de lucro de sus antecedentes y las empresas y entidades -verificadoras de datos, head hunters, agencias de marketing directo, etcétera - que cuentan a su favor con normas que amparan sus prácticas."

Termina dicho acápite, que "De esta forma, la moción pretende resguardar los datos personales-patrimoniales y evitar los abusos que en base a éstos se cometen a diario por algunas empresas dedicadas al giro del procesamiento de datos con fines de lucro."

Bajo el acápite 5 del mensaje, titulado "las necesarias modificaciones a la ley 19.628.", el legislador señala haciendo suyas las opiniones del citado Sr. Jijena, en el sentido que "como principales reparos a la ley vigente: el no contemplar un órgano fiscalizador y la inexistencia de un registro obligatorio de bases de datos; establecer como regla general que los datos personales en Chile son públicos (artículo 2 letra i); definir de forma ambigua los datos sensibles o personalísimos y dejar la calificación de su uso a las propias empresas interesadas -tales como clínicas, ISAPRE, empresas funerarias- en el artículo 10° de la ley 19.628; excluir de su aplicación a las empresas o personas jurídicas (que no pueden ampararse en el Habeas Data); o contemplar un enorme cúmulo de excepciones legales genéricas a los datos que por regla general pueden procesarse sólo en virtud de una autorización legal o del titular de los datos (artículo 4°). Debe entenderse y tenerse presente que ellas no han obedecido a criterios técnico jurídicos sólidos y que no encuentran asidero legal alguno en el Derecho Comparado."[198]

Además, se refiere y justifica la necesidad de protección de los datos "personales" de las personas jurídicas, las que también poseen atributos de su personalidad aunque su naturaleza jurídica emane de una ficción legal. Señala al respecto, que "Son sujetos de información cuyos antecedentes también son "tratados" computacionalmente, y por definición quedan al margen de la ley que expresamente sólo rige en relación a "titulares" personas naturales. Ocurre que la información sobre las personas jurídicas es tan relevante como la de las personas naturales y también merece ser resguardada.

Esta tutela jurídica por ende permanece en el ámbito de las reglas generales del derecho, por lo que cualquier persona jurídica respecto de la

198 JIJENA LEIVA, Renato; "Comercio Electrónico, Firma Digital y Derecho, análisis de la ley 19.799", pag 58 y ss. publicado en Diciembre del año 2002 por la Editorial Jurídica Andrés Bello.

cual se abuse de sus antecedentes propios o bien éstos sean procesados en forma errada (datos obsoletos, caducos, inexactos), deberá recurrir a los procedimientos, acciones y recursos generales contemplados en nuestro ordenamiento jurídico. Estimamos que si bien en menor amplitud que las personas naturales, las personas jurídicas también gozan de un necesario derecho a la confidencialidad o reserva de los antecedentes que a ellas se refieren, por cuanto éstos las convierten en sujetos de derechos y en personas identificadas e identificables."

Posiblemente, muchas de las críticas del legislador, quizás pueden ser atendibles y tener sustento jurídico, pero no necesariamente implica que por ello, la modificación legislativa que se plantea, sea en la dirección correcta.

Hecha dicha exposición, procedamos a revisar el artículo 1° del proyecto, los numerales 1, 2 y 3 se refieren a incorporar a las personas jurídicas a dicha protección. Señala el proyecto de ley que en la ley 19.628 de 28 de agosto de 1999, la protección fue considerada sólo para las personas naturales, omitiéndose expresamente a las personas jurídicas, las cuales en opinión del Senador Novoa, también tienen una intimidad, la cual debe ser resguardada.

En este escenario, el legislador sigue la opción minoritaria en el mundo de incluir a las personas jurídicas, siguiendo el mismo proceso que la legislación de Austria, Dinamarca, Luxemburgo y Noruega que incluyen en la protección de dicha normativa también a las personas jurídicas y en contraposición a la Ley francesa y Española, así como a las directrices de la Unión Europea.

Al respecto, y habiendo revisado la historia de la ley, hay que dejar

establecido que jamás fue intención de los autores y legisladores proteger a las personas jurídicas al respecto, y siempre tuvo como único alcance el proteger la vida privada de las personas naturales.

Si bien, en parte puede tener razón en el sentido de que no tienen la debida protección, aun cuando a su parecer tienen atributos de la personalidad, pero desgraciadamente el exceso de entusiasmo, llega hasta el extremo de proteger a personas jurídicas en integridad física o moral, tal como lo señala expresamente el nº 3 del artículo primero.

Por otra parte se cambia el alcance de los llamados Datos de carácter sensible, incorporándose expresamente la dirección de correo electrónico, los datos respecto a los clientes de las empresas, sus estados financieros, etc.

Además, se modifica la utilización de datos obtenidos de fuentes de acceso público, ya a su parecer son tales las excepciones que la Regla general pierde tal sentido.

En virtud de lo anterior se modifica la letra i) del artículo 2 de la ley 19.628, pues el concepto de fuentes públicas de acceso bastante amplio por una delimitación de dicho concepto, ya que se da una enumeración prácticamente taxativa de los mismos.

En el mismo sentido modifica el art.4 liberando de la autorización del titular de los datos personales, si estos provienen de aquellos señalados en la letra anterior, o aquellos que utilicen las personas jurídicas privadas sin fines de lucro para su propio uso.

Por último se elimina la idea de autorización tacita, por el mero hecho de haber incorporado los datos una persona en un sitio web.

En resumen de lo anterior nos encontramos, que el legislador propone modificar en el art.1 Nº 1 del proyecto el artículo 2º letra f) de la ley 19.628, incorporando expresamente a las personas jurídicas, quedando asi: "Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales o jurídicas, identificadas o identificables.".

El mismo art. Propone en el Nº 2 modificar la definición de Datos de Carácter sensible contenida en el art. 2º letra g), ampliándolo de la siguiente manera: "Datos sensibles, aquella especie de datos personales que aludan a las características físicas o morales de las personas naturales o jurídicas, a hechos o circunstancias que estimen constitutivos de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, la vida sexual, los estados de salud físicos o psíquicos, sus direcciones de correo electrónico, las nóminas de sus clientes y los estados financieros y patrimoniales positivos o no regulados por los artículos 17 y siguientes de esta ley. Su tratamiento computacional o manual sólo será procedente mediando autorización previa y expresa de los titulares a quienes aludan".

También el mismo artículo en su Nº 3 propone modificar la letra i) del citado art. 2, reglamentando las llamadas Fuentes Accesibles al público, señalando: "Constituyen fuentes públicas de información las bases de datos computacionales y los listados manuales cuyo acceso o consulta pueda ser efectuada por cualquier persona, de manera gratuita u onerosa, siempre y cuando ello no esté prohibido por tener el carácter de secretos o reservados, tales como, la estadística de los censos; los listados telefónicos en los términos previstos por su normativa específica; las listas de

personas pertenecientes a grupos de profesionales que voluntariamente se hayan incorporado, consintiendo en el tratamiento público de sus datos, y que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, domicilio o residencia e indicación de su pertenencia al grupo; los diarios y boletines oficiales; los medios de comunicación social; y todas aquellas que revistan tal calidad por haberse registrado, almacenado o tratado los datos personales con el consentimiento previo y expreso del propietario de éstos."

Luego en el número 4, propone sustituir los incisos 5º y 6º del artículo 4º, quedando su redacción como se indica: "Artículo 4°.- El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello. La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público. La autorización debe constar por escrito.

La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito. "No requieren autorización del titular respectivo, únicamente y de manera excepcional, las operaciones de tratamiento de datos personales provenientes de las fuentes accesibles al público definidas en el artículo 2º de esta ley.

Tampoco requerirán de dicha autorización el tratamiento de datos personales que realicen las personas jurídicas privadas, sin fines de lucro, para el uso exclusivo suyo, de sus asociados y de las entidades a que estén afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos".

Finalmente, en lo que respecta a este tema propone reemplazar el art.9 de la ley, por el siguiente: "Los datos personales a que alude la presente ley

deben utilizarse para los fines considerados o declarados por sus titulares al momento de su comunicación, registro o almacenamiento, salvo que provengan o se hayan recolectado de fuentes accesibles al público. Respecto a la recopilación de datos personales de empresas o personas naturales, obtenidos directamente de sitios de la red Internet, de manera alguna podrá entenderse que ha sido otorgada una autorización tácita para su uso con fines diversos a los inherentes a los derivados de la naturaleza o finalidad del sitio".

Por último y siendo consecuente con el nuevo artículo 2 letra g), el legislador propone la creación de un nuevo titulo II a continuación del artículo 9°, "Sobre la protección de los datos sensibles en general y de las direcciones de correos electrónicos en particular", pasando los restantes a ser III, IV, V y VI respectivamente.

En tal sentido el Nº 7 del proyecto propone incorporar el siguiente artículo 10 A: "Artículo 10 A: El dato personal dirección de correo electrónico poseerá la calidad de sensible, y a su respecto sólo procederá el tratamiento manual o computacional del mismo mediando la autorización a que alude al artículo 4º de esta ley, otorgada en forma previa, escrita o electrónica, por la persona natural o por el representante de la persona jurídica a que se refieran y que sean individualizados por dicha dirección. El titular de la dirección de correo electrónico en cualquier momento podrá dejar sin efecto la autorización dada para el envío de los mismos, en cuyo caso el emisor deberá eliminar los datos del destinatario y, en caso de haberlos comunicado a terceros, informarles de la revocación. De manera alguna se podrá entender que el hecho de mantenerse publicada una dirección de correo en un sitio WEB de la red Internet implica el otorgamiento de una autorización tácita para el uso de la misma con fines de promociones comerciales o publicitarias, o para otros diversos a los

inherentes que se deriven de la naturaleza o finalidad del sitio.

En resumen de ello, el legislador pretende en este punto modificar la ley:

1.- Incorporando a las personas jurídicas como titulares de protección de la ley en estudio, al establecerlos como titulares de los llamados "Datos Personales" y al incorpóralos también como sujeto de protección de los llamados datos personales de carácter sensible;

2.- Invierte la técnica legislativa, al modificar las llamadas fuentes publicas de información, al hacer una enumeración prácticamente taxativa, de los casos que podrían entenderse como fuentes de acceso público;

3.- Limita los casos en que no se requiere autorización del titular de los datos, para que puedan ser accedidos por cualquiera, quedando expresamente excluidos todos los datos comerciales, financieros y bancarios, entre otros;

4.- Reafirma el concepto que los datos sólo pueden utilizarse para los fines que hayan sido entregados y elimina la autorización tacita por encontrarse en una página web, y

5.- Incorpora a la Dirección de Correo electrónico como un Dato Personal de carácter sensible.

En mi opinión, y de conformidad a los antecedentes anteriores no nace en parte alguna la necesidad real de dar a la Dirección de Correo electrónico el carácter de Dato Sensible, pues por su estructura y aun cuando por el supuesto análisis de otros antecedentes se pudiera llegar a convertir en sensible, puesto que a ese respecto no hay ningún dato que escape de ello, mas aun que en el evento que se le diera tal carácter, quien sería el

responsable real de la custodia del mismo, ya que podría incluso generar lesiones pecuniarias a los proveedores del servicio de correo, si alguien utiliza en forma ilegitima el email, lo cual como se explica en el anexo técnico, no tiene ninguna dificultad el "casi adivinar" las direcciones de Correo electrónico de las personas.

En cuanto a lo que respecta a la regulación del Spam, hay que partir señalando que el legislador señala que no existe un termino o concepto unánime del anglicismo "spam", pero para efectos de la Moción lo define "todo correo electrónico enviado de forma masiva, sin autorización del titular de la dirección o casilla electrónica, obteniéndose las direcciones de correos de fuentes no públicas de información, y que ocasiona perjuicios económicos al receptor de la comunicación, independientemente de que su contenido se relacione -o no- con una promoción comercial u oferta de servicios".

El legislador propone la creación de un nuevo titulo II a continuación del artículo 9°, "Sobre la protección de los datos sensibles en general y de las direcciones de correos electrónicos en particular", pasando los restantes a ser III, IV, V y VI respectivamente.

En razón de haberse analizado en forma independiente la dirección de correo electrónico como dato sensible, procederemos a analizar los restantes artículos de este numeral 7del proyecto que propone incorporar los siguientes artículos 10 A, B, C, D y E nuevos:

"***Artículo 10 B: El titular de la dirección de correo electrónico podrá requerir y solicitar, a la empresa proveedora de conectividad a la red Internet que preste los servicios de mantención y operación de casilla(s) electrónica(s) tanto al emisor como al receptor de los***

correos, o al que opere como mero transportador, el bloqueo de la dirección del emisor que le envíe un correo no solicitado previamente.
Dicho bloqueo, o la adopción de otras medidas técnicas para filtrar los mensajes como la limitación diaria, semanal o mensual de la cantidad de mensajes enviados por sus usuarios, procederá por el sólo hecho de la solicitud, notificación y/o reclamo que realicen un mínimo de cinco usuarios y sólo respecto de una dirección determinada o no de un rango genérico de direcciones. Realizado el bloqueo bajo estas condiciones no podrá ser considerado denegación de servicio por parte del proveedor del emisor de los correos.
A estos efectos, el proveedor de conectividad deberá implementar un procedimiento claro y expedito, y elaborar y publicar una lista de todas aquellas direcciones a cuyo respecto le sea solicitado bloquear la dirección del emisor, de manera que pueda ser consultada por los sistemas o servidores de correos de otros proveedores."

El presente artículo propuesto incorpora a los proveedores de servicio de emails, la obligación de bloquear aquellas casillas que un usuario nos solicite bloquear, estableciéndose la obligación de crear un procedimiento rápido y expedito al respecto, con lo cual obviamente se esta transfiriendo una mayor responsabilidad al proveedor, como sería pretender que el operador telefónico filtrara las llamadas telefónicas que un usuario no quiere recibir.

Desgraciadamente el sistema, con que actúan quienes manejan bases de datos y envían los llamados spam, es a través de direcciones ficticias o que son cambiadas permanentemente a modo de evitar los filtros, lo cual obviamente podría traer aparejado que para un usuario que nos solicitara por ejemplo bloquear vinosdeexportación@hotmail.com y que envía ofertas todos los días, al día siguiente podría llegar uno de vinos@hotmail.com, y

el nombre que le aparece al usuario ser el mismo, con lo cual para el sería su proveedor el que no tomo las acciones de bloqueo que el solicito.

Por otra parte, al menos la ley se preocupa que cuando un proveedor bloquee a un spamer, no se le considerara en negación de servicios, y oficializa la creación de listas negras para ser utilizadas por todos los proveedores

"Artículo 10 C: Atendida la naturaleza de carácter sensible del dato dirección de correo electrónico, se prohíbe la comercialización anónima y sin autorización previa, escrita o electrónica, del titular del dato, de listas, guías, compilaciones, registros o bases de datos que contengan direcciones de correos. "

"Artículo 10 D: Toda comunicación promocional o publicitaria enviada por correo electrónico o por servicios de mensajería telefónica celular, no solicitada y enviada en forma masiva y reiterativa, deberá: a) indicar en su título o asunto los elementos que reflejen el contenido o motivo del mensaje o la materia o asunto sobre la que versa; b) especificar la identidad del remitente; y c) contener una dirección válida para requerir la suspensión de los envíos, mantenida en el servidor computacional de una empresa ubicada en Chile y que sea claramente identificable. La empresa deberá individualizarse en la comunicación indicando: Nombre o Razón Social, domicilio, RUT, correo electrónico y representante legal.
En caso que el titular requiera la suspensión de los envíos, o no responda, el emisor no podrá enviar nuevas comunicaciones. El emisor sólo podrá enviar una comunicación de este tipo al año, cumpliendo con todos los requisitos señalados en el inciso anterior.

El no cumplimiento de estas normas será considerada infracción a esta ley y a la ley de protección de los derechos de los consumidores."

Al respecto es conveniente señalar, que todo el alcance y análisis que se hace mantiene el supuesto de que se trate de spammers chilenos y situados en servidores dentro de nuestro país, obviando inexplicablemente la extraterritorialidad del Internet y de los servicios de casillas de correos.

"Artículo 10 E: Lo dispuesto en los artículos 16 y 23 de la presente ley se aplicará también a las infracciones al las normas de este título."

Es decir se establecen el procedimiento para seguir las acciones ante los tribunales para recuperar la debida protección, siendo los registros o bancos de datos los responsables de ese hecho, pudiendo ser condenados a multas e indemnizaciones.

A mayor abundamiento dichas normas señalan lo siguiente:

"Artículo 16.- Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente.
El procedimiento se sujetará a las reglas siguientes:
a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de

prueba que los acrediten, en su caso.

b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte.

c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada.

d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos.

Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta.

e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario.

f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes.

h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación.

En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente.

La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública.

En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales.

La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días".

"Artículo 23.- La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá

indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez.

El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

Por último el legislador propone derogar el artículo 28 B de la ley 19.496 (de defensa del consumidor), incorporado en el año recién pasado, que señala "Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos.

Los proveedores que dirijan comunicaciones promocionales o publicitarias a los consumidores por medio de correo postal, fax, llamados o servicios de mensajería telefónicos, deberán indicar una forma expedita en que los destinatarios podrán solicitar la suspensión de las mismas. Solicitada ésta, el envío de nuevas comunicaciones quedará prohibido."

Las razones por la cual se plantea esta derogación, las encontramos en el mismo mensaje de la moción.

En efecto, en la moción se señala que “no es suficiente abordar el problema (el Spam) en el contexto de la ley de derechos de los consumidores, como se ha propuesto y aprobado a esta fecha en Chile mediante la ley N°19.955, modificatoria de la ley 19.496, toda vez que suele no darse entre el emisor del correo electrónico no deseado, invasivo y perjudicial y el receptor del mismo, una relación de aquellas generadas entre proveedores y consumidores que se regulan en el contexto del derecho de los consumidores. Dicho de otra forma, los e-mails que saturan las casillas o buzones de correo electrónico pueden no contener ofertas, promociones comerciales o publicidad engañosa y no ser emitidos por proveedores que ofertan un bien a cambio de un precio.”

Reconoce la moción, que “Si bien, de esta forma, se trató de paliar el problema del spam en la modificación a la ley del consumidor señalada más arriba, sabíamos que ésta no estaba exenta de problemas en su aplicación práctica y que, por tanto, la materia requería ser perfeccionada en la ley que ahora se propone modificar. Por ejemplo, el hecho de que uno solicite ser removido de una base de datos, no hace sino comprobar al emisor que el receptor tiene la casilla activa, lo que valoriza su base de datos. Además, al solicitar ser removido, aparece una dirección que lleva a registrarse en una base de datos de un país extranjero en donde la ley chilena no tiene ninguna posibilidad de ser aplicada. Ello ha permitido que se generen cientos de "primeros envíos" de ofertas de distintos productos y desde direcciones diversas, con la posibilidad sólo teórica de ofrecer una posibilidad de removerse que, en general, resulta ser ineficaz.”

Finalmente señala “que, lamentablemente, la “autorregulación” promovida por la SUBTEL y por la entidad gremial que agrupa a los proveedores de

internet ha resultado ineficaz, debido, fundamentalmente, a que se trata de simples sugerencias o recomendaciones que nadie está obligado a cumplir. “

Finalmente y en otro orden de ideas la moción del Senador Novoa, atenta contra los principios básicos del Derecho Informático, los cuales según la opinión de diversos profesores, son la concreción de la Garantías y con el fin de concluir con este capítulo podemos señalar respecto de este proyecto,:

1.- La RATIO JURIDICA que se ha pretendido seguir, no obedece a ningún criterio objetivo atendible, ya que al incorporar la DIRECCION DE CORREO ELECTRONICO como dato sensible en el artículo 2 letra g) y Artículo 10 A, no se esta atendiendo a lo que ha sido la tendencia mundial en la materia, de que se trate de datos que puedan generar con su mal uso o tratamiento, una discriminación hacia el afectado.

2.- Tal como se señalo, en la actualidad a través del tratamiento de datos, ya sea manual o automático, el problema reside que existe tal cúmulo de información, que hasta el dato mas inofensivo, se puede convertir en una bomba de tiempo.

3.- Al no existir una Ley de Datos Personales acorde a la experiencia internacional, cualquiera sea el carácter que se le de a determinados datos, de nada sirve, toda vez que si la ley no es clara en el mecanismo de protección, no define a cabalidad cual es el objeto o finalidad de la recogida del dato, si no existe un control de la autoridad respecto del tratamiento de datos, que a su vez impide que se pueda ejercer el derecho de información y consentimiento, no existirá jamás una “autodeterminación informativa” y una posibilidad real de ejercer el

Habeas Data.

4.- En lo que respecta al Spam, la moción parlamentaria, sencillamente pretende derivar toda la responsabilidad en contra de los proveedores de Internet y del servicio de correos, en circunstancias, que son tan o mas afectados que los usuarios que reciben estas comunicaciones no deseadas, gravando una actividad legitima, con verdaderas sanciones, al tener que permanentemente estar invirtiendo en nuevos equipos, personal y estudios para poder intentar lograr hacer lo que pretende el legislador

5.- El sistema de sanción impuesto, implica colocar a los ISP o MSP en una situación de permanente peligro ante los usuarios, cada vez que pretendan utilizar los sistemas de reclamo, ante un bloqueo solicitado, principalmente por el hecho del analfabetismo digital imperante en los tribunales de justicia.

6.- El legislador también olvida el problema de la aterritorialidad, que hace perder toda eficacia a cualquier intento de regulación o sanción, toda vez que un spammer nacional, lo primero que hará será contratar un servidor fuera de las fronteras de Chile.

7.- El pretender establecer por vía de una simple modificación legal, que el proveedor aplique “filtros” sobre los correos, ya que ello trae aparejado el hecho de que se intervenga el mensaje técnicamente y se abra y revice su contenido, lo que implica una violación al artículo 19 Nº 4 y 5 de la Constitución Política, ya que en ninguna parte se establece que estas garantías sólo pueden ser conculcadas por personas y no por maquinas.

8.- Finalmente, la moción olvida los principios de derecho que están involucrado en un asunto como este, los cuales son simplemente extensiones de las garantías fundamentales de las personas, en su actuar

en el mundo real y no virtual.

Este Proyecto actualmente se encuentra en estado de ser enviado a la Comisión de Economía del Senado, según acuerdo adoptado en agosto de 2007.

E-. Proyecto Carlos Ominami y Jaime Naranjo

Con fecha 1 de octubre de 2008, fue ingresado un nuevo proyecto sobre la materia en estudio, el cual tiene por objeto modificar las leyes Nº 19.496, y Nº 19.628 con el objeto de regular el envío de correos electrónicos y de llamadas o "spams" telefónicos de carácter comercial y/o publicitario[199]; cuya autoría es de los Honorables Senadores Carlos Ominami y Jaime Naranjo.

En la exposición de fundamentos, se comienza destacando el actual papel de la Internet, tanto a nivel mundial como nacional, señalando el nivel de penetración de esta en Chile, equivalente a un 35% de la población.
Continúa, que esta penetración, coloque a la población chilena en una exposición continua a la red, tanto por computadoras como por equipos de telefonía móvil; poniéndose a disposición de los consumidores a "gran velocidad" publicidad de la más variada y a costos bajísimos, especialmente a través de correos electrónicos.

Se destaca el hecho, que en los últimos años se ha dado al correo electrónico usos ilegales o al menos ilícitos, citándose las practicas de envío masivo e indiscriminado de mensajes de correo electrónico no

[199] BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 6136-03 . [en línea] Chile. [Fecha de consulta: 17 Diciembre 2008] Actualización permanente. Disponible en: http://www.bcn.cl/

deseados, de carácter comercial publicitarios, es decir, Spam.

Se señala, que una de las consecuencias que trae dicha actividad es el empobrecimiento injusto que sufre el usuario de Internet, ya que por el envío indiscriminado de correos, y la administración de las redes de los proveedores, se pueden ver incrementado sus costos de conexión y por consiguiente las tarifas.

En el punto 5 de la exposición de fundamentos se señalan las consecuencias que trae aparejada esta actividad; indicándose:

"a) El envío masivo de estos correos produce una disminución importante en el ancho de banda de las redes, un uso intensivo de servidores cuyos materiales y componentes se desgastan con mayor rapidez y un consumo de energía muy importante por parte de dichos servidores. Asimismo, los proveedores de servicios de internet deben invertir importantes recursos materiales y humanos para la eliminación de este tipo de correos, así como para la implementación, mantención y actualización de filtros adecuados para prevenir que este tipo de prácticas pueda inutilizar los servicios tecnológicos.

b) Los proveedores de servicios de Internet deben asumir los costos derivados de las consecuencias adversas asociadas a este tipo de prácticas. Sin embargo, para poder seguir brindando el servicio, dichas entidades traspasan el aumento en sus costos de operación al usuario final quien debe soportar esta alza, encareciendo el acceso a la banda ancha.

c) El creciente aumento de los spam, de la más variada naturaleza, implica que los buzones de los particulares se vean atiborrados de

estos mensajes. De esta manera, el e-mail termina convirtiéndose en una molestia, llevando al usuario a buscar canales alternativos de comunicación que se encuentren libres de mensajes indeseados y que por lo general son más costosos, inseguros y lentos.

d) Generalmente de estos correos vienen asociados a virus informáticos o software de código malicioso, que pueden provocar daños en los sistemas infectados. Del mismo modo, el anonimato en el que operan quienes inician la transmisión permite llevar a cabo con relativa facilidad determinados delitos especialmente ligados al ámbito de las defraudaciones y al comercio sexual."

Previo a continuar el análisis, es importante señalar, que de todos los proyectos anteriores, este es el primero donde existe "aparentemente" una preocupación global del problema; ya que siempre el legislador ha buscado proteger al usuario, y no ha considerado en los efectos, a los demás actores del negocio, principalmente los proveedores de red y de servicio de correo electrónico, que efectivamente sufren las consecuencias señaladas previamente.

Dije "aparentemente" en el párrafo anterior, ya que de la redacción del proyecto, queda claro que esa preocupación, sólo quedo en la exposición de motivos, ya que en la normativa no se realmente reflejada dicha preocupación; pues no queda claro en forma directa, la posibilidad del proveedor de red o de servicio de Correo Electrónico, de perseguir al spammer por medio de acciones indemnizatorias, pero al menos puede servir para abrir el debate y el abanico de posibilidades una vez que se comience la discusión del proyecto.

Otro punto importante del proyecto y que señala en la exposición previa,

es la ampliación del concepto Spam, al Spam telefónico, siguiendo la corriente internacional. La razón como se señala al terminar los fundamentos y se explica por si sola ***"En nuestro país, existen un poco más de 3 millones de líneas telefónicas, las que, según datos de la autoridad, todas han recibido una llamarada no deseada de carácter publicitario o promocional. La idea del proyecto es dar una regulación a este tipo de mensajes, teniendo como norte siempre el respeto de las personas, su intimidad, incentivar una competencia leal entre las empresas y desincentivar el uso de prácticas moletas, desleales y engañosas."***

En cuanto al proyecto mismo, esté parte por derogar el actual inciso 1º del artículo 28B de la ley Nº 19.496[200] (aun cuando el proyecto señala erróneamente la ley Nº 19.946[201]), reemplazándolo por la siguiente redacción:

"La realización de publicidad o de propuestas comerciales de bienes y servicios, por vía telefónica de red fija o móvil, fax u otro medio de comunicación a distancia, sólo podrá hacerse cuando el titular de la línea telefónica de red fija o el suscrito a un plan de telefonía móvil o el dueño del teléfono móvil, hayan expresa e inequívocamente consentido en ello al tiempo del contrato, o en un acto posterior, y aún en este caso, la publicidad y propuestas aludidas en este inciso, sólo podrá efectuarse en días u horas hábiles.

Con todo, cuando el titular de una línea de red fija, o suscrito a un plan de telefonía móvil o dueño de un teléfono móvil, consintiera en recibir publicidad o propuestas comerciales, podrán siempre y en cualquier tiempo pedir el cese, para lo cual los proveedores deberán indicar una manera expedita y gratuita para solicitar la suspensión

---

[200] Establece Normas Sobre Protección de los Derechos de los Consumidores, Publicada en Diario Oficial 7 Marzo 1997 y modificada por Ley Nº 19.955 Publicada en Diario Oficial 14 Julio 2004.

[201] Modifica la ley austral en materia de crédito tributario y establece la ampliación de la zona franca de extensión de Punta Arenas a la región de Aise n para bienes de capital.

de los envíos. Una vez hecha esta solicitud, los envíos de publicidad o de propuestas comerciales quedarán suspendidas.
Lo anterior no obsta a que los usuarios soliciten nuevamente el envió de publicidad o de propuestas comerciales.
La infracción a lo dispuesto en este artículo será sancionada con las multas previstas en el artículo 34 C de este proyecto."

Con la norma expuesta parte la moción incorporando expresamente la regulación de las comunicaciones comerciales telefónicas no solicitadas. Estableciendo un sistema de opt In, ya que solo se pueden enviar a los usuarios que se hayan previamente inscrito para recibir dichas ofertas.

Al respecto hay que citar que el anterior proyecto del Senador Naranjo, que buscaba regular las llamadas publicitarias por teléfono, establecía el sistema contraria, ya que decía expresamente en el inciso segundo del artículo que reemplazaría el actual 28B; "***Así mismo se deberá implementar un Registro Nacional donde las personas dueñas de teléfonos fijos y celulares dejaran establecido su voluntad de no recibir llamados telefónicos publicitarios de cualquier tipo. La inscripción en este registro será gratuita y durará 5 años. Las empresas que realicen publicidad mediante esta vía deberán obligatoriamente consultar este registro."***[202]

En relación al envío de correos electrónicos, el proyecto contempla incorporar en la Ley Nº 19.496 un párrafo completo, a fin de regular el envío de estos, bajo el nombre de ***"Limitaciones al envío de correos electrónicos de carácter comercial y/o publicitario".*** Este párrafo

[202] BCN. Biblioteca del Congreso Nacional de Chile. Boletín Nº 4844-06 . [en línea] Chile. [Fecha de consulta: 17 Diciembre 2008] Actualización permanente. Disponible en: http://www.bcn.cl/

contiene 6 artículos, que intentan abarcar la problemática completa del Spam.

El artículo 34 A parte por establecer el principio de consentimiento del receptor de correo electrónico. Al efecto, señala:

"Toda comunicación comercial o publicitaria enviada por correo electrónico deberá ser consentida previamente por el destinatario.
Se entenderá que el destinatario ha consentido la recepción de comunicaciones comerciales o publicitarias remitidas por correo electrónico, cuando:
a) Haya manifestado expresamente su intención de recibir dichas comunicaciones, sea en respuesta a una solicitud planteada de manera clara y asertiva o bien, sea por propia solicitud del destinatario; y
b) Haya sido informado claramente al momento de prestar su consentimiento, que su dirección de correo electrónico podría ser entregada a la parte por cuya cuenta se inicia la transmisión del correo electrónico de carácter comercial o publicitario, si la comunicación proviene de una parte distinta de aquella a la cual el destinatario ha manifestado su consentimiento.
Se entenderá por destinatario, a toda persona que recibe un correo electrónico comercial no solicitado."

De la redacción anterior, podemos observar que se abandona el actual sistema opt out, vigente en la ley chilena, y se establece un sistema de inclusión, al igual como se propone con las comunicaciones comerciales telefónicas.

Obviamente, la inclusión del sistema opt In, si bien puede significar un problema mayor para quienes ejercen válidamente el telemarketing o

prospección comercial, debiera en principio suponer una disminución de los correos electrónicos no solicitados. Desgraciadamente, este requisito solo afectara a quienes realicen lícitamente hasta el día de hoy prospecciones comerciales, ya que para los spammers y su demostrado desprecio hacia los receptores de correo, no parece ser un tema que los vaya a intimidar.

Continúa el artículo 34 B, estableciendo los requisitos que debe contener un correo electrónico comercial o publicitario, señalando al efecto:

"El Correo Electrónico Comercial o publicitario deberá contener y exhibir de forma sencilla, clara y completa:

a) Una descripción breve, precisa y representativa del contenido del correo electrónico y la palabra "publicidad"; "anuncios"; "circulares"; "ofrecimiento"; "propuesta"; o "invitación", en el campo del objeto o asunto

b) Datos de identificación del emisor, incluyendo nombre y apellido o razón social, domicilio físico, teléfono y dirección de correo electrónico, así como iguales menciones respecto del proveedor de bienes o prestador de servicios por cuyo encargo se inicia la transmisión del mensaje, cuando se trate de una persona distinta del remitente.

Se entenderá por emisor a la persona quien inicia un mensaje y cuyo producto, servicio o sitio de INTERNET es anunciado o promocionado por el mensaje.

c) Un vínculo o una dirección de correo electrónico válida a la que el destinatario pueda solicitar, expedita y gratuitamente, la suspensión de los envíos, que quedarán desde entonces prohibidos. Dicho vínculo o dirección deberá mantenerse vigente por, al menos, 30 días después de haberse enviado el mensaje; y

d) Tratándose de publicidad o anuncio de productos y servicios para

mayores de edad, las comunicaciones respectivas sólo podrán ser enviadas a destinatarios que hayan prestado consentimiento previo de manera expresa de conformidad con lo dispuesto en el artículo 34 A. En estos casos, el proveedor de bienes o servicios deberá implementar y aplicar sistemas, dispositivos o mecanismos idóneos para constatar que el destinatario que ha prestado su aceptación, es mayor de edad. Tales mensajes deberán incluir en la sección "asunto" la frase "PUBLICIDAD PARA MAYORES DE EDAD".

Continúa el señalado proyecto, estableciendo en el Artículo 34 C, el régimen infraccional, al tenor de la siguiente redacción:

"Comete infracción a las disposiciones de esta ley toda persona que envíe correos electrónicos de carácter comercial o publicitario, a sabiendas o debiendo saber la concurrencia de alguna de las siguientes circunstancias:

a) Cuando no se cuente con la autorización del destinatario o en dicha comunicación no se hubiere cumplido con los requisitos establecidos en el artículo 34 B, o

b) Cuando contenga información falsa respecto de la persona del remitente o del proveedor de bienes o prestador de servicios, por cuya cuenta se inicia la transmisión que impida su adecuada identificación por parte del destinatario del mensaje, o

c) Cuando el "asunto" de dicho mensaje contenga información falsa, errónea o que induzca a error o engaño, en relación a los bienes o servicios ofrecidos.

d) Cuando la persona del remitente o del proveedor de bienes o prestador de servicios, por cuya cuenta se inicia la transmisión, engañe para disfrazar el origen de los mensajes o que se registre con direcciones electrónicas diferentes utilizando información falsa para enviar correos electrónicos comerciales.

El engaño se define como la alteración del encabezamiento o de la

información de ruta.
Las infracciones señaladas serán sancionadas con multa de 5 unidades tributarias mensuales a 500 unidades tributarias mensuales y, en caso de reincidencia, con multa de 10 unidades tributarias mensuales a 1.000 unidades tributarias mensuales"

La norma en comento detalla, las posibles infracciones que se pueden cometer, ya sea por falsedades, engaños, falta de rigurosidad en el envío, etc; tratando de especificar el máximo de situaciones posibles en que se pueda cometer la infracción. Desgraciadamente, dicha norma comete un grave error, en su primer párrafo ya que establece "la concurrencia de al menos una de las circunstancias", debiendo haberla dejado a modo ejemplar, pues aun cuando aparentemente no hay ninguna otra posibilidad de infracción que las indicadas, no olvidemos que hablamos de una ley eminentemente tecnológica, y no se debe olvidar nunca la evolución de la informática y tecnologías de la información, y aun hoy hagamos esfuerzos sobre humanos para imaginarnos en que situación podría quedar sin aplicación esta ley, no lo conseguiremos, pero si tenemos la certeza de que más temprano que tarde, se abrirán las alamedas por donde pasará el spammer libre.

El art 34 D, continúa con el régimen infraccional, aplicando las mismas multas establecidas en la norma anterior, para quienes realicen las practicas que en este se establecen:
"Con las mismas multas señaladas en el artículo anterior será sancionada toda persona que, con ocasión de la comisión de alguna de las conductas establecidas en el artículo precedente, incurriere en alguna de las siguientes prácticas:
a) Obtuviere direcciones de correo electrónico de terceros a través de medios automáticos, aplicaciones o software desarrollados o

adaptados para la recolección masiva de direcciones de correo electrónico a través de Internet o mecanismos automáticos, aplicaciones o software basados en el empleo de combinaciones, letras o números, con ese propósito, o

b) Utilice líneas o comandos de programación u otros medios automáticos para registrar múltiples cuentas de correo electrónico a través de las cuales inicie la transmisión, o
c) Utilice listados de direcciones de correo electrónico obtenidas mediante el empleo de los mecanismos descritos en las letras a) o b) anteriores, o
d) Cuando la respectiva comunicación incluya o vaya acompañada de nombres de dominio, marcas, información, productos o servicios de terceros, sin el consentimiento del titular, en la sección "asunto" o en el cuerpo mismo del mensaje con el propósito de confundir al destinatario, sin perjuicio de las acciones de los titulares de dicha información, con arreglo a la ley Nº 17.336 y 19.039, según corresponda, o
e) Se valga de cualquier mecanismo o técnica de carácter manual o automático para eludir un sistema de filtro o bloqueo o medida tecnológica de protección, implementada."

Queda de manifiesto que se refiere a sancionar todas las actividades de cosecha de casillas de correos electrónicos y similares. En este caso, insisto en lo mismo que en el artículo anterior, la necesidad que en la redacción del primer párrafo, sea incorporando la frase "entre otros", aun cuando la letra e) pueda considerarse un cajón de sastre; pero desgraciadamente la imaginación es ilimitada, sobre todo para violar la ley o cometer fraudes, o simplemente por el animo de muchos hackers de violar un sistema por mera entretención o desafío personal.

El proyecto, en el artículo 34 E, parece acordarse de los proveedores de servicio de Internet y/o correo, ya que le entrega un par de facultades.

En efecto, señala la norma en comento, en su inciso primero:

"Los proveedores de servicios de Internet o de servicios de correos electrónicos, podrán establecer programas, sistemas o mecanismos que permitan filtrar o bloquear las comunicaciones comerciales o publicitarias masivas. Dichos proveedores de servicios deberán informar a los usuarios finales, de manera clara y oportuna, de la existencia de tales mecanismos o dispositivos, sus alcances, y efectos."

Lo anterior implica, que los proveedores puedan lícitamente utilizar filtros, aplicaciones u otro softwares, que impidan la recepción de spam, siempre y cuando informan a los usuarios. Este tema no es menor, ya que la forma de operar de los filtros anti spam, es por medio de la apertura y lectura automatizada de los correos electrónicos, en busca de determinados caracteres o contenidos en el interior del mensaje, lo cual en estricto rigor sería atentatorio contra la privacidad de la comunicación. El problema que la protección y garantía de la inviolabilidad de las comunicaciones es una garantía con consagración constitucional, y mal podría ser modificada por intermedio de una simple ley.

Una segunda facultad que le entrega la ley a los proveedores, es la de bloqueo, contenida en los incisos segundo y tercero del artículo 34 E, la que señala:
"Sin perjuicio de lo que dispongan los términos y condiciones de los servicios proveídos, tras recibir un aviso adecuado de parte del destinatario, el proveedor de servicios de Internet o de correo

electrónico respectivo podrá bloquear el acceso al servicio, suspender y cancelar las cuentas de aquellos usuarios que hayan sido condenados por sentencia judicial ejecutoriada dictada en procedimiento infraccional seguido de conformidad con las normas de la presente ley. En estos casos, el proveedor no será responsable de los resultados producidos por el filtro o bloqueo de los mensajes de correo o por el bloqueo, suspensión o cancelación de la cuenta de un usuario.

Se entenderá por "aviso adecuado" el remitido por el destinatario de un mensaje de correo electrónico de carácter comercial o publicitario, a través de cualquier medio, con indicación de su nombre completo, dirección física y de correo electrónico y que contenga en el cuerpo del aviso respectivo un historial o extracto del mensaje enviado en contravención a las normas del presente párrafo, así como los datos contenidos en el mismo, respecto del remitente de dicho mensaje."

Este derecho de bloqueo, sin duda, es una garantía para el proveedor, ya que ***bloquear el acceso al servicio, suspender y cancelar las cuentas de aquellos usuarios que hayan sido condenados por sentencia judicial ejecutoriada***, válidamente a quien realice actividades de spam; siempre y cuando le sea solicitado por el destinatario de estos mensajes. Pero que ocurre, con aquellos emisores que sean denunciados y que no hayan sido condenados por sentencia judicial ejecutoriada. ¿Se creara un registro de spammers condenados?, ¿se pondrá a disposición de los proveedores de Internet o de servicio de correos electrónicos?, ya que de la redacción de la norma no queda claro como operara el sistema. De acuerdo a la norma, si un usuario solicita el bloqueo el proveedor debiera estar obligado a hacerlo; pero si no hay constancia de la condena y no lo hace, el usuario podría intentar iniciar acciones en contra del proveedor.

Por otra parte los artículos 34 F y 34 G, se encargar de reglamentar las acciones de indemnización de perjuicios, textos que se bastan por si solos, y que señalan literalmente:

"Artículo 34 F. Los afectados por el envío de correos electrónicos enviados con infracción a las normas establecidas en el presente párrafo, podrán ocurrir ante el juez de policía local respectivo con arreglo al procedimiento infraccional contemplado en el Título IV de la presente ley a fin de que el Tribunal ordene el cese de la actividad ilícita, la imposición de multas y la indemnización de los daños y perjuicios causados.

Las acciones de indemnización de perjuicios podrán ser ejercidas en contra de toda persona natural o jurídica que inicia la transmisión del mensaje así como de toda persona natural o jurídica que reciba un beneficio patrimonial efectivo a consecuencia del envío del mismo, por los destinatarios de los mensajes de correos electrónicos no autorizados de carácter comercial o publicitario, así como por los proveedores de servicios de Internet o de correo electrónico.
Lo previsto en este artículo será aplicable a lo dispuesto en el artículo 28 B."

"Artículo 34 G. Sin perjuicio de lo dispuesto en el inciso 7º del artículo 50, serán considerados para los efectos de cálculo del monto de la indemnización que proceda, especialmente:
a) La cantidad de mensajes transmitidos por el infractor en una determinada red ya sea a través de una o de múltiples cuentas de correo electrónico empleadas para tal efecto;
b) La congestión y disminución efectiva en el ancho de banda de la red a consecuencia de la transmisión de dichos mensajes;

c) Si para posibilitar el envío de dichos mensajes, el infractor ha incurrido en alguna de las conductas descritas en el artículo 34 D; y
d) El beneficio patrimonial percibido por el infractor o por el beneficiario de la publicidad cuando el mismo sea atribuible de manera directa o indirecta a la infracción.
Para los efectos contemplados en el presente artículo, salvo prueba en contrario, se presumirá que inicia la transmisión del mensaje, el titular de la cuenta de correo electrónico señalada como remitente de dicho mensaje. De la misma manera, se presumirá que percibe un beneficio patrimonial efectivo a consecuencia del envío de dichos mensajes, la persona por cuya cuenta son publicitados los bienes y servicios singularizados o referidos en dichos mensajes."

De lo anterior, queda claro que el titular de las acciones del artículo 34 F, se refiere tanto al destinatario afectado como los ISP o MSP, lo cual permitirá intentar resarcir los perjuicios sufridos por las mayores inversiones realizadas para evitar los daños o para reparar daños en sus redes; sin que ello signifique un aumento de costo para el usuario.

Finalmente, no podemos negar que este proyecto, sin duda constituye un avance, respecto a la actual legislación, así como respecto de los otros proyectos, y que aun cuando queda mucha tela que cortar, debiera convertirse en una ley adecuada, siempre y cuando los legisladores, estén decididos a escuchar a todos a quienes realmente afecta este problema y no solo a los organismos de gobierno o asociaciones de consumidores.

V.- CONCLUSIONES: PASOS A SEGUIR PARA OBTENER UNA REGULACIÓN EFICAZ DEL CORREO ELECTRÓNICO NO DESEADO EN CHILE.

Habiendo concluido el análisis técnico y legal, tanto en Chile como a nivel Internacional del Correo Electrónico no deseado y toda su problemática, es de suma importancia, llevar las naves a puerto, y para ello, es necesario analizar que debiéramos hacer en Chile para lograr frenar el SPAM, con el fin de disminuirlo y en un mediano plazo extinguirlo casi por completo.

Para ello, sin duda, estamos frente a una labor casi titánica, ya que implica muchas acciones coordinadas, tanto a nivel nacional como internacional, y eso obviamente lo hace aun mas difícil todavía.

Estas acciones, necesariamente tienen mucho que ver con lo revisado y analizado latamente en el capítulo III de este trabajo, y son a saber:

A.- Contenidos mínimos de un proyecto de ley sobre el tema
B.- Explicitación de la garantía constitucional del número 5 del articulo 19
C.- Promoción y suscripción de tratados internacionales
D.- Modificación de la agenda digital.

Además en opinión de este autor, el problema no pasa por perseguir los Correos Electrónicos comerciales no deseado, el problema es proteger la intimidad de las personas y por ello, una ley debe considerar toda clase de comunicación no deseada, sin importar si es comercial o su pasividad; y en tal sentido como anexo final al presente trabajo, adjunto un proyecto de modificación de ley, el cual se ha basado en parte en la actual moción de los senadores Ominami y Naranjo, ya comentado.

A.- Contenidos mínimos de un Proyecto de Ley sobre el tema

Como primer punto abordaremos la elaboración de un proyecto de Ley que regule expresamente esta materia, la cual no necesariamente debe ser una Ley exclusiva sobre el Correo electrónico, sino que perfectamente podría ser parte de una Ley Marco que regule las comunicaciones electronicas no deseadas.
Este proyecto de ley, debiera contemplar una serie de normas, que sirvieran de guía para todos quienes quieran hacer de esta actividad, una actividad lícita y sobre todo como una herramienta de protección eficaz a los miles de usuarios en Chile.

En tal sentido dicho proyecto debiera contemplar:

a.- Conceptos

Obviamente se deberá explicitar los conceptos de:

a.1 Comunicación electrónica

a.2 Comunicación electrónica no deseado

Respecto de este último es sumamente importante que se hable de **"Comunicación electrónica no deseada",** sin limitarla con la expresión **"comercial",** ya que como hemos visto, hoy en día no necesariamente, un correo basura o invasivo de la privacidad de los usuarios es necesariamente comercial, sino que tal como ya se ha señalado majaderamente, existen estas comunicaciones, igualmente desagradables y que no obedecen a una actividad de prospección comercial, sino que política, religiosas, gremiales, y un sin numero de etcéteras.

Por otra parte, también e excluido expresamente el término **"masivo"**, pues aparte de ser un término sumamente subjetivo, ya que para saber cuándo lo podremos considerar masivo es muy difícil, y obviamente dejaría abierta la puerta para defensas ante las autoridades, basadas en la cantidad, tal como ocurre muchas veces con las leyes de drogas, que exculpan a quien son sorprendidos con drogas para su consumo personal y no para comercializar.

Por último respecto del concepto de correo electrónico no deseado, y atendida la actual globalización y convergencia de redes, que el concepto se haga extensivo a todo tipo de comunicaciones electrónicas, fijas o móviles, con lo cual se podría dar la misma protección a los usuarios de telefonía fija o móvil o a los múltiples usuarios de servicios de mensajería instantánea; con lo cual, adicionalmente, estaríamos ampliando la protección hacia los grupos de adolescentes y niños, muy asiduos a estas mensajerías y por lo mismo mas expuestos.

b.- Excepción.

Al respecto y a contrario sensu, deberá reglamentarse a titulo de excepción las actividades licitas de prospección comercial, conocidas hoy como e-marketing.

Obviamente, y así como hicimos hincapié, en que el concepto de correo electrónico, no debiera contener el concepto comercial como limitativo, acá lo ideal sería referirnos a prospección publicitaria; entendiendo por publicidad **"es un esfuerzo pagado, trasmitido por medios masivos de información con objeto de persuadir"**[203], siendo esté último termino el

203 O´Guinn Tomas, Allen Chris y Semenik Richard, Publicidad. International Thomson Editores, Pág. 6

que nos permite ampliar el concepto a la venta o promoción de cualquier idea. En este sentido otros autores, incorporar expresamente el concepto "idea", en efecto, ya que se dice también que la publicidad es "**una comunicación no personal, pagada por un patrocinador claramente identificado, que promueve ideas, organizaciones o productos."**[204]

Hecha dicha aclaración, podemos continuar, estableciendo las características que tendrían estas comunicaciones excepcionales, y que requisitos deberán cumplir para ser catalogadas de tal y no ser consideradas como correo no deseado.

Para ello se deberá establecer que sistema de autorización será valido en Chile para el envío de correos o comunicaciones electrónicas con este fin, es decir, si establecemos un sistema de exclusión o uno de inclusión. En ambos casos, obviamente, se deberá establecer la obligatoriedad de provenir de una casilla de correo electrónico valida y que el emisor sea absolutamente identificable, así como los requisitos para la remoción de las listas y un sistema simple de identificación del tipo de comunicación, de manera que a quienes no les interese, con sólo ver el asunto del correo puede decidir inmediatamente la eliminación del mismo y solicitar su remoción.

Finalmente, respecto de este punto se deberán establecer las sanciones a quien viole estas disposiciones, posiblemente remitiéndose a la parte en particular que sanciones todas las comunicaciones ilícitas o no deseadas.

c.- Protección usuarios

Para llevar a cabo la protección efectiva de los usuarios, se deberá

204 Stanton William, Etzel Michael y Walker Bruce, Mc Graw Hill. Fundamentos de Marketing, 13a Edición, Pág. 569

establecer un procedimiento, que permita de manera eficaz intentar las acciones, tanto administrativas o judiciales según sean los casos, a fin de obtener las sanciones e indemnizaciones que se establezcan.

En este sentido, se deberá establecer que autoridad será competente para conocer y fallar estas acciones judiciales y/o administrativas, dotándolos de la suficiente facultad de imperio, de manera de poder cumplir o hacer cumplir sus sanciones.

En este orden de cosas, para aquellos casos en que nos mantengamos ante acciones de carácter meramente administrativas, será necesario establecer una autoridad contralora, que pueda conocer de todas las denuncias que hagan los usuarios que se vean afectados por estas comunicaciones, de manera que ellos sancionen directamente aplicando multas que pudieran ser procedentes, o que inicien ante los tribunales ordinarios de Justicia competentes, las acciones civiles de indemnización o criminales que pudieren corresponder, en atención al tipo de comunicación enviada y al eventual daño causado o delito aparejado que pudiere llevar.

No se debe olvidar en este punto, que es muy importante que no exista duplicidad de autoridades, que eventualmente puedan conocer de estas materias, como ocurre en otros países en que es competente una autoridad contralora de datos y los servicios de defensa de los consumidores.

d.- Exención de responsabilidad de los proveedores de acceso a la red o comunicaciones electrónicas.

Este tema es un punto no menor, en un sistema de comunicación que tiene muchas aristas o actores.

Si bien, siempre se ha buscado establecer una ley en este sentido para proteger a los usuarios, como la parte más débil del sistema; también no es menos cierto que los proveedores de acceso a la red o a las comunicaciones, también se van perjudicados o dañados por estas prácticas. Los perjuicios, no sólo se presentan por el hecho de que se saturen las redes perjudicando a todos los usuarios, al verse colapsadas las mismas, bajando las velocidades de conexión, o teniendo que invertir en programas para evitar estas acciones, etc. Tal como se señalaba anteriormente, en relación a las legislaciones internacionales, ya que se protege al proveedor de servicios de correo electrónico, cuyas políticas respecto de la publicidad no solicitada enviada por correo electrónico sean violadas, de manera que pueda iniciar las acciones civiles pertinentes para reclamar indemnizaciones por los daños y perjuicios sufridos por dicha violación, siempre y cuando, haya este, previamente a la violación alegada, haber notificado fehacientemente al demandado sobre sus propias políticas de publicidad no solicitada enviada por correo electrónico.

Además, es necesario permitir lícitamente a los responsables del servicio o proveedor de acceso a no responder por el bloqueo que impidan a solicitud de sus clientes la recepción o la transmisión de cualquier comunicación no deseada a través de sus sistemas o sin consentimiento en que aparezca de manifiesto que se viola la ley.

e.- Régimen sancionatorio

Tal como se señalo anteriormente, se deberán establecer sanciones adecuadas y que de una manera traigan aparejada, el carácter correctivo de la misma y que corresponda a la realidad de la acción misma.

En este sentido deberán establecerse multas crecientes, pero cuya base

parta siendo una suma considerable, que al Spammer o a quien lo contrata para enviar su correos, no le resulte atractiva dicha actividad.

Además, se deberán establecer sanciones civiles reparatorias, que permitan indemnizar a los usuarios o proveedores que se vean afectados con el actuar de los spamers.

Adicionalmente, se deberán establecer las sanciones penales, a que se puede ver expuestos quienes hayan sufrido la comisión de algún delito, aparejado a estas actividades ilícitas, a través de un correo electrónico; siempre y cuando que dicha acción típica, no se encuentre expresamente contemplada o incorporada al catalogo penal general del país.

f.- Modificación de otros cuerpos legales para la adecuación a esta.

Al respecto existen una serie de cuerpos legales, que deberán ser modificados para completar esta ley, y que le permita operar correcta o eficientemente.

En primer lugar, habría que modificar la Ley de Defensa de los Derechos de los Consumidores Nº 19.496, a fin de derogar el artículo 28 B, incorporado por la ley 19.955, que intento sancionar el Spam, y que como ya se ha dicho, su efecto no ha sido eficaz, por decir lo menos.

En segundo lugar, sería sumamente importante establecer la incorporación o el establecimiento de una autoridad contralora, que sea competente para velar por la protección de los usuarios, para lo cual sería razonable, la modificación de la **Ley 19.628, SOBRE PROTECCIÓN DE LA VIDA PRIVADA O PROTECCIÓN DE DATOS DE CARÁCTER.**

PERSONAL[205].

En efecto, la referida ley, no ha podido hasta el día de hoy obtener la aplicación real para efectiva resguardar la intimidad de las personas, ya que carece de una autoridad contralora, como ocurre en España, entre otro lugares. Dicha autoridad, que en España es la Agencia Española de Protección de Datos, tiene competencias especificas respecto del Spam con contenido comercial, tanto para investigar las denuncias recibidas como para sancionar las posibles infracciones que se encuentren tras el oportuno procedimiento de investigación; pudiendo incluso sancionar directamente a Spammers tanto en España como en el resto de UE, que afecten con sus actividades a usuarios en España, estableciendo en general sendas multas que oscilan entre los 30.000 y 600.000 euros.

Hay que hacer presente que hoy se encuentra en primer trámite legislativo una modificación a la Ley 19.628 y a la **LEY 20.285**[206]**, SOBRE ACCESO A LA INFORMACIÓN PÚBLICA** en el sentido de incorporar al Consejo para la Transparencia establecido en dicha ley, como autoridad contralora, entregándole la función de velar por el adecuado cumplimiento de la normativa sobre protección de datos personales, por parte de organismos públicos y personas naturales, o jurídicas de carácter privado, junto con establecer un sistema único nacional de registro de los bancos de datos personales.

En otro orden de cosas, se debiera modificar el Código Penal, incorporando la **LEY Nº 18.223 SOBRE DELITOS INFORMÁTICOS**[207], la cual obviamente debe desaparecer, e incorporando dentro del Código mencionado, las distintas conductas típicas que puedan ir acompañadas

205 Publicada en el Diario Oficial de 28 de agosto de 1999
[206] Publicada en el Diario Oficial el 20 de agosto de 2008
207 Publicada en el Diario Oficial el 7 de junio de 1993

del Spam o afines a ella, y que fueron tratadas en el capítulo II de este trabajo, y que en general, son de una u otra manera, distintas formas de cometer fraudes, los cuales debieran incorporarse en los artículos correspondientes, así como los que tienen por objeto amenazas, prostitución o pornografía infantil, etc.

Demás está decir que se requerirá hacer las adecuaciones que sean necesarias, a los Códigos de Procedimiento, en el sentido de valorar los correos electrónicos, aun cuando no contengan firma electrónica avanzada, de manera de poder hacer factible procedimientos de protección y reparación para usuarios y proveedores. Por las mismas razones debiera modificarse la **Ley Nº 19.799 SOBRE DOCUMENTO ELECTRÓNICO, FIRMA ELECTRÓNICA Y LOS SERVICIOS DE CERTIFICACIÓN DE DICHAS FIRMAS**, por cuanto sus actuales normas, no bastan para este objeto.

En definitiva, modificar o adaptar todos los cuerpos legales de nuestro país que requieran esta actualización, para la correcta aplicación de una ley sobre esta materia.

B.- Interpretación extensiva de la Garantía Constitucional del número 5 del artículo 19 respecto de los correos electrónicos

Hasta hace poco tiempo, la mayoría de las personas no consideraba, como objeto de protección a las comunicaciones contenidas en Correos electrónicos, o mejor dicho que no eran parte de la Garantía constitucional del Artículo 19 Nº 5.

La verdad que hoy parece ser obvio, el alcance de dicha norma, y ya nadie discutiría que dichas comunicaciones están debidamente amparadas. En el Derecho Comparado, por ejemplo el profesor mexicano Miguel Carbonell ha señalado en relación a la misma garantía en la Constitución mexicana y redactada en términos similares que "hace una referencia general, sin distingos de ninguna índole, a la naturaleza de las comunicaciones y de la forma en que éstas se presentan; no se restringe la disposición constitucional sólo a los escritos impresos, sino que el concepto alcanza a cualquier grabación que en medios electrónicos, ópticos o digitales se realice, incluyendo, las que se generen mediante el uso de de tecnologías como Internet"[208]

En Chile, si bien no han surgido acciones al respecto y que hayan sido difundidas masivamente, existen actos administrativos que así lo han reconocido, tal como el Dictamen Nº 0260/019 de 24 de enero de 2002 de la Dirección del Trabajo, la cual con ocasión de los correos electrónicos de los trabajadores señalo que el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, **PERO EN NINGÚN CASO PODRÁ TENER ACCESO A LA CORRESPONDENCIA ELECTRÓNICA PRIVADA ENVIADA Y RECIBIDA POR LOS TRABAJADORES.** Estas facultades de administración del Correo electrónico el empleador la tiene por aplicación de la Garantía Constitucional del Nº 26 del artículo 19, ya que esta establece que las regulaciones legales de una garantía constitucional autorizadas por la propia Constitución, "no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio"; lo cual obviamente ocurriría si se limitara la facultad de

208 Carbonell, Miguel, Los Derechos Fundamentales en México, México, Universidad Nacional Autónoma de México, 2004, pp. 139-140

dirección y administración del empleador.

Establecida la extensión de la garantía respecto de las comunicaciones electrónicas, se debe establecer expresamente dentro de las excepciones la posibilidad de conocer, aunque sea "lógicamente" su contenido, de manera que puedan ser analizados sus contenidos, de manera que se libere de responsabilidad de una supuesta acción anticonstitucional, a los proveedores que a fin de proteger sus redes y a sus clientes instalen sistemas lógicos o mecánicos, para filtrar las comunicaciones enviadas, de manera de eliminar los Spam, ya que en estricto rigor, estos sistemas incurrirían en violación de la garantía constitucional del Nº 5 del artículo 19 de la Constitución Política, ya que estos sistemas aun cuando en forma imperceptible, la manera de operar es abriendo el correo o leyéndolo, buscando determinadas características, que permiten determinar de antemano que dicha comunicación por parte de su contenido es un Spam.

C.- Promoción y suscripción de Tratados Internacionales

Este punto quizás a esta altura es el mas obvio, y posiblemente el mas difícil de obtener, ya que implica la alineación internacional con este tema. Tal como se vio en un capítulo anterior, con ocasión de las experiencias internacionales, en especial de Europa, la Comunidad Europea, ha intentado uniformar las legislaciones y suscribir acuerdos que permitan de otra manera soslayar todos los problemas que trae el envío de correos electrónicos no deseados.

Estos tratados son de suma importancia, pues como bien saben todos, existe un elemento no menor para lograr obtener una real protección de

los usuarios, esta es la extraterritorialidad de la red; en el sentido que los correos que se reciban en Chile, no necesariamente tendrán su origen en nuestras fronteras.

Por ello, que se requiere para que funcione nuestra ley, así como la de los otros países, es de suyo importancia la colaboración y comunicación internacional, de modo tal que la diferencia de jurisdicción no obstaculicen la persecución de estas prácticas.

Para ello, se requiere de tratados de cooperación internacional, como lo que ocurre con los acuerdos de las distintas Policía, las cuales cooperan unas con otras.

En atención a ello, sería dable y aconsejable instar por un Tratado o acuerdo Internacional, que establezca procedimientos comunes para la denuncia de spammers que hayan actuado en los respectivos países y que el origen de las comunicaciones se encuentre fuera de las fronteras; crear sistemas de listas negras comunes que si bien hoy se hace, pero por una iniciativa de los privados y no de los Estados; en general a toda clase de intercambio de comunicaciones que puedan ayudar a frenar esta práctica.

Finalmente, respecto a este punto, y posiblemente lo mas difícil será aunar los criterios de que se sancionara en cada Estado, donde sin duda existirán diferencias gravitantes.

D.- Modificación de la Agenda Digital.

Finalmente, y como último grupo de acciones, se encuentran aquellas destinadas al usuario en general, y que debieran ser incorporadas a la Agenda Digital, como una etapa siguiente a la llamada alfabetización

digital, pues según se señalaba en la introducción del documento denominado "***Agenda Digital***[209]" su objetivo era ***"contribuir al desarrollo de Chile mediante el empleo de las tecnologías de información y comunicación (TIC) para incrementar la competitividad, la igualdad de oportunidades, las libertades individuales, la calidad de vida y la eficiencia y transparencia del sector público, enriqueciendo al mismo tiempo la identidad cultural de la Nación y de sus pueblos originarios. Las TIC no son un fin en sí mismas. Son instrumentos para modernizar el Estado, incrementar la productividad y acortar las diferencias entre grandes y pequeñas empresas, mejorar la eficiencia de las políticas sociales, disminuir las disparidades regionales de desarrollo y aumentar la equidad. De esta forma, la Agenda Digital busca poner a las TIC al servicio de estos objetivos nacionales".***

Obviamente, si lo que se busca en buscar igualdad entre los distintos actores de la sociedad, debemos educar a la gente, que ya ha accedido al mundo on line, que sepa cómo cuidarse ella, cuidar a sus hijos, y en general cuidar este Derecho al Acceso, que si bien en Chile aun no obtiene rango constitucional como garantía; como todo bien, es un bien escaso. Se debe instruir y enseñar a utilizar filtros de correo en los propios computadores, el Gobierno puede realizar acciones a fin de que se descarguen, instalen y utilicen softwares libre, abundantes en la red, de manera que cada usuario, tome la iniciativa de protegerse, de que se

209 Es el resultado de un trabajo iniciado en abril del año 2003 con la constitución del Grupo de Acción Digital (GAD), presidido por el Coordinador Gubernamental de Tecnologías de Información y Comunicación, y un grupo público-privado conformado por instituciones de gobierno, organizaciones representativas del ámbito empresarial, sector académico y de otros poderes del Estado.
Con fecha 17 de marzo de 2004 se entrego al Presidente de la República los 34 puntos que contemplaba la Agenda Digital 2004-2006, el cual constituye un amplio acuerdo público-privado sobre una estrategia-país, mirando a la celebración del Bicentenario en 2010, y un Plan de Acción para el período 2004-2006, que contemplaba 34 iniciativas separadas en 6 puntos principales.

respeten las garantías constitucionales respecto de ellos, y que realmente surja el convencimiento, que somos libres y que esa libertad comprende nuestro derecho a la privacidad e inviolabilidad de las comunicaciones.

ANEXO

Propuesta de Ley que establezca una reglamentación a las Comunicaciones Electrónicas no deseadas

Artículo 1

Se entenderá por comunicación electrónica, para los efectos de esta ley, entre otras las siguientes:

a) Los Correos electrónicos
b) Los mensajes cortos de telefonía móvil
c) Las llamadas telefónicas vía a operadora o sistema de audiotexto
d) Los mensajes desplegados en los sistemas de comunicación instantánea
e) En general todos aquellos en que se utilice para la envío y/o transmisión del mensaje redes de comunicaciones públicas o abiertas

Artículo 2

El envío de toda comunicación comercial, publicitaria o promocional, a una persona, deberá ser previamente consentida por este.

Artículo 3

Se entenderá por comunicaciones comerciales, publicitarias o promocionales no deseadas a aquellas que contenga información, falsa o real, dedicada a la promoción o publicidad, directa o por cuenta de terceros, de bienes o servicios de una persona jurídica o natural, que realice una actividad comercial, industrial, artesanal o profesional, o

cualquier otra actividad con fines lucrativos.
Asimismo, también se considerara para los efectos de esta ley como comunicaciones comerciales, publicitarias o promociónales aquellas que contengan promoción o publicidad, directa o por cuenta de terceros, de organizaciones políticas o religiosas, así como cualquiera otra que promueva todo tipo de ideologías, pensamientos o corrientes de opinión.

Artículo 4

Se entenderá que el destinatario ha consentido en la recepción de comunicaciones comerciales, publicitarias o promocionales, cuando:

a) Ha manifestado expresamente su intención de recibir dichas comunicaciones al solicitarlo expresamente;
b) Ha manifestado expresamente su intención de recibir dichas comunicaciones al responder una solicitud planteada en forma clara y asertiva;
c) Ha autorizado expresamente a quien haya hecho entrega de sus datos de contacto, a transferirlos o cederlos a uno o mas terceros.

Se deja expresamente establecido, que no se entenderá comprendido en los casos anteriores, a los destinatarios que hayan publicado sus datos de contacto, tales como direcciones de correo electrónico, número telefónicos, etc en sitios de libre acceso como paginas web, salones de Chat, guías telefónicas o similares.

Artículo 5

Toda comunicación comercial, publicitaria o promocional, deberá contener y exhibir sencilla, clara y completa la siguiente información:

a) Una descripción breve, precisa y representativa del objeto del contenido de la comunicación, seguido por la palabra "publicidad"; "anuncios"; "circulares"; "ofrecimiento"; "propuesta"; "invitación", “doctrina”; o “ideología” en el campo del objeto o asunto tratándose de correos electrónicos o al inicio o encabezado de la comunicación.

b) Datos de identificación del emisor, incluyendo nombre y apellido o razón social, domicilio físico, teléfono y dirección de correo electrónico, así como iguales menciones respecto del tercero, por cuyo encargo se inicia la transmisión del mensaje, cuando se trate de una persona distinta del remitente.

c) Un vínculo o una dirección de correo electrónico válida, así como una número telefónico sin costo para el destinatario de la comunicación, a fin de que este pueda solicitar, expedita y gratuitamente, la suspensión de los envíos, que quedarán desde entonces prohibidos. Dichos vínculos, direcciones o números telefónicos, deberán mantenerse vigente por, al menos, 30 días después de haberse enviado el mensaje; y

d) Tratándose de publicidad o anuncio de productos y servicios para mayores de edad, las comunicaciones respectivas sólo podrán ser enviadas a destinatarios que hayan solicitado expresamente el envío de las comunicaciones, de conformidad a la letra a) del artículo 4º. En estos casos, el emisor deberá contar con sistemas, dispositivos o mecanismos idóneos y eficaces para constatar que el destinatario que ha prestado su aceptación, es mayor de edad. Tales mensajes deberán incluir en la sección “**asunto**” o al comienzo de la comunicación de la frase “PUBLICIDAD PARA MAYORES DE EDAD”.

Artículo 6

Serán consideradas como infracciones a la presente ley, las cometidas por toda persona que envíe comunicaciones comerciales, publicitarias o promocionales, en contravención a los contenidos de la presente ley.
Se consideraran como comunicaciones comerciales, publicitarias o promocionales, en contravención a la presente ley, entre otras:

a) Cuando no se cuente con la autorización del destinatario de conformidad con el artículo 4

b) Cuando no cumpla con los requisitos establecidos en el artículo 5

c) Cuando contenga información falsa respecto de la persona del remitente o del tercero, por cuya cuenta se inicia la transmisión que impida su adecuada identificación por parte del destinatario del mensaje,

d) Cuando el "asunto" o el inicio o el encabezado de la comunicación contenga información falsa, errónea o que induzca a error o engaño, en relación a los bienes o servicios ofrecidos o ideas que se pretende difundir.

e) Cuando la persona del remitente o del tercero, por cuya cuenta se inicia la transmisión, engañe para ocultar el verdadero origen de las comunicaciones o que se registre con datos diferentes utilizando información falsa para enviar comerciales, publicitarias o promocionales.

Artículo 7

También serán consideradas como infracciones a la presente ley, las actividades de toda persona que, con ocasión de la comisión de alguna de las conductas establecidas en el artículo precedente, incurriere en alguna

de las siguientes prácticas:

a) Obtuviere direcciones de correo electrónico, números telefónicos, direcciones de servicios de mensajería instantánea de terceros, a través de medios manuales o automáticos, aplicaciones o software desarrollados o adaptados para la recolección masiva de dichos datos a través de Internet y de toda clase de redes de comunicaciones o mecanismos automáticos, aplicaciones o software basados en el empleo de combinaciones, letras o números, con ese propósito, o

b) Utilice líneas o comandos de programación u otros medios automáticos para registrar múltiples cuentas de correo electrónico a través de las cuales inicie la transmisión, o

c) Utilice listados de direcciones de correo electrónico, de mensajería instantánea, de números telefónicos obtenidos mediante el empleo de los mecanismos descritos en las letras a) o b) anteriores, o

d) Cuando la respectiva comunicación incluya o vaya acompañada de nombres de dominio, marcas, información, productos o servicios de terceros, sin el consentimiento del titular, en la sección "asunto", inicio, encabezamiento o en el contenido mismo del mensaje con el propósito de confundir al destinatario, sin perjuicio de las acciones de los titulares de dicha información, con arreglo a la ley Nº 17.336 y 19.039, según corresponda, o

e) En general se valga de cualquier mecanismo o técnica de carácter manual o automático para eludir un sistema de filtro o bloqueo o medida tecnológica de protección, implementada, ya sea por el destinatario o por los proveedores de los servicios de comunicaciones.

Artículo 8

Las personas que incurran en una o más de las acciones descritas en los artículos 6 y 7 de la presente ley, serán sancionadas con multa de 5 unidades tributarias mensuales a 500 unidades tributarias mensuales por cada una de las infracciones cometidas y, en caso de reincidencia, con multa de 10 unidades tributarias mensuales a 1.000 unidades tributarias mensuales por cada una de las infracciones cometidas.
Los terceros que contraten los servicios de envío de comunicaciones comerciales, publicitarias o promocionales, serán condenados solidariamente con el emisor de la misma.

Artículo 9

Los proveedores de servicios de Internet, de servicios de correos electrónicos, de servicio telefónico y en general de comunicaciones, podrán establecer programas, sistemas o mecanismos que permitan filtrar o bloquear las comunicaciones comerciales, publicitarias o promocionales. Dichos proveedores de servicios deberán informar a los usuarios finales, de manera clara y oportuna, de la existencia de tales mecanismos o dispositivos, sus alcances, y efectos.

Sin perjuicio de lo que dispongan los términos y condiciones de los servicios proveídos, tras recibir un aviso adecuado de parte del destinatario, el proveedor de servicio respectivo se encontrará facultado para bloquear transitoriamente el acceso al servicio, hasta por un plazo de 30 días corridos, salvo que en el intertanto el destinatario solicitante del bloqueo acredite haber iniciado las acciones legales en contra del emisor.

En el evento que el emisor resulte condenado como autor de alguna de las infracciones establecidas en la presente ley, el proveedor del servicio se

encontrará facultado para bloquear definitivamente el servicio.

En estos casos, el proveedor no será responsable de los resultados producidos por el filtro o bloqueo de las comunicaciones o por el bloqueo, suspensión o cancelación de la cuenta de un usuario.

Se entenderá por "aviso adecuado" el remitido por el destinatario de una comunicación comercial, publicitaria o promocional, a través de cualquier medio, con indicación de su nombre completo, dirección física y de correo electrónico y que contenga en el cuerpo del aviso respectivo un historial o extracto del mensaje enviado en contravención a las normas de la presente ley, así como los datos contenidos en el mismo, respecto del remitente de dicho mensaje.

Artículo 10

Conocerá de las infracciones cometidas en violación de las disposiciones de la presente ley, el juez de policía local respectivo con arreglo al procedimiento que se dictara dentro del plazo de 60 días de entrada en vigencia la presente ley, a fin de que el Tribunal ordene el cese de la actividad ilícita, la imposición de multas y la indemnización de los daños y perjuicios causados.

Artículo 11

Las acciones de indemnización de perjuicios podrán ser ejercidas en contra de toda persona natural o jurídica que inicia la transmisión del mensaje así como de toda persona natural o jurídica que reciba un beneficio patrimonial efectivo a consecuencia del envío del mismo, por los destinatarios de las comunicaciones comerciales, publicitarias o

promocionales, así como por los proveedores de servicios afectados por la emisión de las señaladas comunicaciones.

Artículo 12

La presente ley entrara en vigencia 120 días después de su publicación en el Diario Oficial, a fin de que los interesados puedan implementar las medidas necesarias para asegurar el efectivo cumplimiento de la presente ley.

DECLARACION DEL AUTOR

El autor señala que al cierre definitivo de este trabajo, todas las citas, que incluyen direcciones de Internet, fueron visitadas, accedidas y actualizadas al día 1 de Agosto de 2009, verificándose su acceso.

BIBLIOGRAFIA

- Agencia de Control de Datos de Española. https://www.agpd.es/index.php
- Antispam brasil. http://www.antispam.br/
- Asociación Peruana Antispam. http://www.antispam.org.pe/
- Bello, Marisa Bello; Irabien Chedraui, José Fernando. El SPAM: un problema real. Revista de Derecho Informático
- No. 055 - Febrero del 2003. http://www.alfa-redi.org/rdi-articulo.shtml?x=1375
- Blum, Lucia Helena. Spam à luz do Código de Defesa do Consumidor. Revista de Derecho Informático. Nº. 045 - Abril del 2002. http://www.alfa-redi.org/rdi-articulo.shtml?x=1538
- Can-Spam Act. http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm
- Chaves, Carolina As diversas faces do Spam. Revista de Derecho Informático
- No. 062 - Septiembre del 2003.http://www.alfa-redi.org/rdi-articulo.shtml?x=1291
- Congreso Nacional de Chile. Proyecto de Ley que busca modificar la ley Nº 19.628 sobre "Protección de datos de carácter personal" para introducir el concepto de uso indebido o abusivo de datos. (boletín Nº 3095-07) http://sil.congreso.cl/pags/index.html
- Congreso Nacional de Chile. Proyecto de ley sobre comercialización y publicidad por medio de redes de telecomunicaciones e internet. Boletín Nº 3094-19. http://sil.congreso.cl/pags/index.html
- Congreso Nacional de Chile. Proyecto que modifica la ley nº 19.628 en lo que se refiere a la publicación de boletines con información de datos personales-patrimoniales, con el objeto de proteger mas adecuadamente

los derechos de las personas y de las pymes. Además, propone modificar la ley para dar una mejor protección a los "datos sensibles" y hacerse cargo de los problemas derivados del "spam" http://sil.congreso.cl/pags/index.html

- Constitución Política de la República de Chile.
- Copani, María. Primer caso judicial en el país contra el envío de correo basura por Internet. http://www.clarin.com/diario/2003/11/21/s-04501.htm
- De la Maza Gazmuri, Iñigo. El Correo en los Tiempos de Internet. .Revista de Derecho Informático. Nº. 047 - Junio del 2002. http://www.alfa-redi.org/rdi-articulo.shtml?x=1493
- Diaz Garcia, Alexander . Sentencia sobre SPAM en Colombia. Revista de Derecho Informático. Nº. 061 - Agosto del 2003. http://www.alfa-redi.org/rdi-articulo.shtml?x=1302
- Elías, Miguel S.. Situación legal de los datos de carácter personal frente a las nuevas tecnologías. REDI Revista Electrónica de Derecho Informático - Número 32 (Marzo de 2001)
- http://premium.vlex.com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Situacion-legal-datos-caracter-personal-frente-nuevas-tecnologias/2100-107859,01.html
- Farinella, Favio. El correo electrónico y el spam, sometidos a una consulta sobre su regulación. Revista de Derecho Informático. Nº. 041 - Diciembre del 2001. http://www.alfa-redi.org/rdi-articulo.shtml?x=1005
- Federal Trade Comission. "Remove Me" Responses and Responsibilities: Email Marketers Must Honor "Unsubscribe" Claims. http://www.ftc.gov/bcp/conline/pubs/alerts/remvalrt.htm.
- Federal Trade Commission. All Email Users: What You Need to Know About Chain Emails & Letters. http://www.ftc.gov/bcp/conline/pubs/online/emailusers.htm

- Federal Trade Commission. CAN-SPAM Act: Requirements for Commercial Emailers. http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm
- Federal Trade Commission. Chain Emails: Just Another Ploy or the Real McCoy? http://www.surfinthespirit.com/the-web/chain.html.
- Federal Trade Commission. Don't Want Your Email Address Harvested? http://www.ftc.gov/bcp/conline/pubs/online/dontharvest.htm
- Federal Trade Commission. Email Address Harvesting: How Spammers Reap What You Sow. http://www.ftc.gov/bcp/conline/pubs/alerts/spamalrt.htm.
- Federal Trade Commission. Keep Your Email Address Unlisted: There Is No "National Do Not Email Registry". http://www.ftc.gov/bcp/conline/pubs/alerts/dnealrt.htm
- Federal Trade Commission. Privacy: Tips for Protecting Your Personal Information http://www.ftc.gov/bcp/conline/pubs/alerts/privtipsalrt.htm
- Federal Trade Commission. Privacy: What You Do Know Can Protect You. http://www.ftc.gov/bcp/conline/pubs/alerts/privprotalrt.htm.
- Federal Trade Commission. Ready to Pop Your Top Over "Pop Up Spam?" Here's How to Make it Stop. http://www.ftc.gov/bcp/conline/pubs/alerts/popalrt.htm
- Federal Trade Commission. Unsolicited Mail, Telemarketing and Email: Where to Go to "Just Say No" . http://www.ftc.gov/bcp/conline/pubs/alerts/optoutalrt.htm
- Federal Trade Commission. Who's Spamming Who? Could it Be You?. http://www.ftc.gov/bcp/conline/pubs/alerts/whospamalrt.htm
- Federal Trade Commission. You've Got Spam: How to "Can" Unwanted Email. http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm
- Fonseca Martínez Claudia. El SPAM y el ejercicio de la Libertad en la

Red. Revista de Derecho Informático. No. 081 - Abril del 2005. http://www.alfa-redi.org/rdi-articulo.shtml?x=956

- Fonseca Martínez Claudia. La Cultura de la Ciberseguridad: indispensable elemento para el desarrollo de los pueblos con menor desarrollo. Revista de Derecho Informático. No. 084 - Julio del 2005. http://www.alfa-redi.org/rdi-articulo.shtml?x=1591.
- Fonseca, Claudia. Comentario a la "Ley que regula el uso del correo electrónico comercial no solicitado (SPAM)", del Perú SPAM, http://www.alfa-redi.org/ar-dnt-documento.shtml?x=812
- Fonseca, Claudia. Comentarios a los Proyectos de Ley en Materia de Control del SPAM y Regulación del Uso del Correo Electrónico en la Nación Argentina SPAM. http://www.alfa-redi.org/ar-dnt-documento.shtml?x=811
- Fonseca, Claudia. Normativa Vigente de SPAM. Centroamérica SPAM. http://www.alfa-redi.org/privacidad/documento.shtml?x=4332
- Fonseca, Claudia. Normativa Vigente de SPAM. Norteamérica SPAM, http://www.alfa-redi.org/privacidad/documento.shtml?x=4331
- Fonseca, Claudia. Normativa Vigente de SPAM. Sudamérica SPAM, http://www.alfa-redi.org/privacidad/documento.shtml?x=4330.
- Graham, James Más vale tarde que nunca.... Revista de Derecho Informático
- Edición: No. 061 - Agosto del 2003 http://www.alfa-redi.org/rdi-articulo.shtml?x=1297,
- Graham, James. Spamming and Law : the European Common Position on E-commerce. Revista de Derecho Informático. No. 022 - Mayo del 2000. http://www.alfa-redi.org/rdi-articulo.shtml?x=466
- Guillén Catalán, Raquel. SPAM y Comunicaciones Comerciales No Solicitadas. Revista Aranzadi de Derecho y Nuevas Tecnologías.
- Internacional Telecommunication Union (ITU). A Comparative analysis of Spam. Law: The quest for model law.

http://www.itu.int/osg/spu/cybersecurity//docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf

- Iriarte Ahon, Erick . Violencia en Internet, ¿Quién defiende a los Internautas?. Sobre el abuso del Correo Electrónico. Revista de Derecho Informático. Nº. 006 - Enero del 1999http://www.alfa-redi.org/rdi-articulo.shtml?x=208
- Jurisprudencia de los Tribunales Norteamericanos http://www.spamlaws.com/cases/index.shtml.
- Leon Leon, Carlos. Consideraciones Legales Relativas al Envío de E-mails Comerciales No Solicitados. Revista de Derecho Informático. Nº. 036 - Julio del 2001. http://www.alfa-redi.org/rdi-articulo.shtml?x=730
- Ley Nº 18.223 sobre Defensa del Consumidor y modificaciones posteriores.
- Machado Vianna, Cynthia Semiramis. Spam: uma abordagem crítica. Revista de Derecho. No. 049 - Agosto del 2002. http://www.alfa-redi.org/rdi-articulo.shtml?x=1468
- Moraes e Silva Neto, Amaro. Um Mundo non sense – e legislações ainda mais... Revista de Derecho Informático. Nº. 061 - Agosto del 2003. http://www.alfa-redi.org/rdi-articulo.shtml?x=1301
- Oruna Rodrigez, Abel Marcial. ¿Regular la Publicidad en el Ciberespacio? Análisis de la Ley que regula el uso del correo electrónico comercial no solicitado (SPAM). Revista de Derecho Informático
- No. 089 - Diciembre del 2005. http://www.alfa-redi.org/rdi-articulo.shtml?x=3915
- Peyrano F. Guillermo. Nuevas problemáticas del tratamiento de datos personales. El tratamiento de informaciones que proporcionan datos persona. REDI Revista Electrónica de Derecho Informático - Número 58 (Mayo de 2003)

- http://premium.vlex.com/doctrina/REDI-Revista-Electronica-Derecho-Informatico/Nuevas-problematicas-tratamiento-datos-personales-tratamiento-informaciones-proporcionan-datos/2100-185296,01.html
- Reinaldo Filho, Democrito Short commentaries on the can-spam ACT. Revista de Derecho Informático.
- No. 070 - Mayo del 2004. http://www.alfa-redi.org/rdi-articulo.shtml?x=1093.
- Ribas Alejandro, Xavier. Aspectos Jurídicos del Comercio Electrónico en Internet. Aranzadi Editorial.
- Sobrino, Waldo Augusto Roberto .Las Cookies y el Spam (y la violación de la Privacidad y la Intimidad). Revista de Derecho Informático. No. 035 - Junio del 2001 http://www.alfa-redi.org/rdi-articulo.shtml?x=710
- Spam laws. http://www.spamlaws.com/
- Stop Spam Alliance. http://stopspamalliance.org/?m=200610
- Ustaran, Eduardo. Data Protection and Electronic Direct Marketing. Revista de Derecho Informático. No. 028 - Noviembre del 2000.http://www.alfa-redi.org/rdi-articulo.shtml?x=575