UNIVERSIDAD NACIONAL DE LOJA

MODALIDAD DE ESTUDIOS A DISTANCIA

CARRERA DE DERECHO

"NECESIDAD DE REFORMAR LA LEY DE COMERCIO ELECTRÓNICO CON LA FINALIDAD DE ESTABLECER UNA PENA CONTRA LOS MENSAJES DE DATOS DE COMUNICACIÓN NO SOLICITADA DE PRODUCTOS Y SERVICIOS"

Tesis previa a la obtención del Título de Abogada.

Autora:

Mayra del Carmen Ruiz Falconí

Director:

Dr. Mg. Marcelo Armando Costa Cevallos

Loja – Ecuador

2014

CERTIFICACIÓN

Dr. Mg. Marcelo Armando Costa Cevallos, DOCENTE DE LA MODALIDAD DE ESTUDIOS A DISTANCIA DE LA UNL.

CERTIFICO:

Que he dirigido y revisado prolijamente el presente trabajo de investigación titulado **"NECESIDAD DE REFORMAR LA LEY DE COMERCIO ELECTRÓNICO CON LA FINALIDAD DE ESTABLECER UNA PENA CONTRA LOS MENSAJES DE DATOS DE COMUNICACIÓN NO SOLICITADA DE PRODUCTOS Y SERVICIOS"**, presentado por la postulante Mayra Ruiz (poner nombre completo) ha sido dirigido y revisado por mi persona; y, en razón de considerar que el mencionado trabajo cumple con los requisitos de fondo y forma establecidos en los reglamentos correspondientes, autorizo su sustentación.

Loja, diciembre del 2014

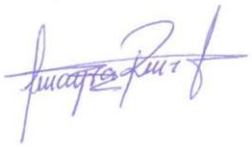
Dr. Mg. Marcelo Armando Costa Cevallos
DIRECTOR DE TESIS

AUTORÍA

Yo, **Mayra del Carmen Ruiz Falconí,** declaro ser Autora del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido del mismo.

Adicionalmente acepto y Autorizo a la Universidad Nacional de Loja, la Publicación de mi Tesis en el repositorio de la Institución- Biblioteca Virtual.

AUTOR: Mayra del Carmen Ruiz Falconí

FIRMA: 

CEDULA: 060224193-7

FECHA: Loja, diciembre del 2014.

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo. Mayra del Carmen Ruiz Falconí, declaro ser autor de la tesis titulada: **"NECESIDAD DE REFORMAR LA LEY DE COMERCIO ELECTRÓNICO CON LA FINALIDAD DE ESTABLECER UNA PENA CONTRA LOS MENSAJES DE DATOS DE COMUNICACIÓN NO SOLICITADA DE PRODUCTOS Y SERVICIOS"** Siendo requisito para optar por el grado de: ABOGADA: Autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja, para que con fines académicos, muestre al mundo la Producción Intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 11 días del mes de diciembre del dos mil catorce.

FIRMA:

AUTOR: Mayra del Carmen Ruiz Falconí

CEDULA: 060224193-7

DIRECCION: Riobamba, San Francisco, Av. Almagro 2148 y 10 de Agosto

CORREO ELECTONICO: mruizf@yahoo.es

TELEFONO: 032963060 - 0996123877

DATOS COMPLEMENTARIOS

DIRECTOR DE TESIS: Dr. Marcelo Acosta Cevallos, Mg. Sc.

TRIBUNAL: Dr. Mg. Augusto Patricio Astudillo Ontaneda

Dr. Mg. Felipe Neptalí Solano Gutiérrez

Dr. Mg. Igor Eduardo Vivanco Müller.

AGRADECIMIENTO

Quiero dejar constancia de mi profundo agradecimiento a todos quienes de una u otra manera coadyuvaron para alcanzar con éxito las metas propuestas.

De manera particular a la Universidad Nacional de Loja en las personas de sus directivos, profesores y personal que labora en tan prestigiosa institución quienes mantienen viva la misión y visión para la que fue creada, al permitir que tantas personas accedan a una educación de calidad.

Quiero dejar constancia de un especial agradecimiento al Dr. Mg Marcelo Armando Costa Cevallos Director de la presente investigación, quien con mucha paciencia ha sabido guiar sabiamente la realización del presente trabajo.

Mayra

DEDICATORIA

- A las personas que me dieron la vida mis padres: Oswaldito Ruiz Chávez (+) , Zoilta Falconi
- Mis hijos, Keevin, Danielita y Mayrita razón sustantiva de mi vida
- Mi hermano querido Oswaldo quien ha sido la persona quien me apoyo para mi culminación
- César compañero de siempre

LA AUTORA

TABLA DE CONTENIDOS

1. TÍTULO

“NECESIDAD DE REFORMAR LA LEY DE COMERCIO ELECTRÓNICO CON LA FINALIDAD DE ESTABLECER UNA PENA CONTRA LOS MENSAJES DE DATOS DE COMUNICACIÓN NO SOLICITADA DE PRODUCTOS Y SERVICIOS”

2. RESUMEN

Actualmente lo conocemos como “spam” o correo “no deseado”, a todo tipo de comunicación no solicitada, realizada por vía electrónica.

De esta forma se entiende por spam cualquier mensaje de datos 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 mediante el correo electrónico.

Esta conducta considero que es gravísima y excesivamente incomoda cuando se realiza en forma masiva.

Esta práctica no se encuentra estipulada dentro de las infracciones informáticas reguladas por la Ley de Comercio electrónico, que se encuentra vigente en el Ecuador, en donde existen reformas al Código Penal en cuanto a ésta clase de infracciones nada se habla en el Ecuador. Sin embargo de ello en muchas legislaciones esto ya se encuentra regulado por ejemplo en la Ley Orgánica de Protección de Datos en España.

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

Constituye para mi punto de vista una vulneración del derecho a la intimidad, tomando en cuenta que la dirección de correo electrónico, así como el número asignado para el celular, pueden y deben ser consideradas como datos de carácter personal.

2.1. ABSTRACT

Today we know it as "spam" or "junk mail", all kinds of unsolicited communication by electronic means.

This means spam is any unsolicited data message and usually has to offer, trade or attempt to arouse interest in a product, service or business. Although you can do in various ways, the most used among the general public is by email.

This behavior think it is too serious and uncomfortable when carried in bulk.

This practice is not stipulated in computer-related offenses regulated by the Law on Electronic Commerce, which is in force in Ecuador, where there are amendments to the Criminal Code regarding this kind of infractions anything spoken in Ecuador. However it many laws that are already regulated by example in the Organic Law on Data Protection in Spain.

The low cost of sending via internet (e-mail) or by mobile phone (SMS), possible anonymity, speed of reaching the target and the potential volume of transmissions, have allowed this practice is carried abusively and indiscriminate.

It is to my view a breach of privacy, considering that the email address and the number assigned to the phone, can and should be regarded as personal data.

3. INTRODUCCIÓN

La Constitución de la República del Ecuador, respecto a los deberes primordiales del Estado señala:

"Art. 3.- Son deberes primordiales del Estado:

…. 8. Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción"

Respecto a los derechos de libertad, la Constitución señala en su Art. 66:

"Art. 66.- Se reconoce y garantizará a las personas:

…..18. El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona.

….19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

20. El derecho a la intimidad personal y familiar.

21. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este

derecho protege cualquier otro tipo o forma de comunicación."

Como se puede ver claramente estipulado dentro de los derecho de libertad se encuentra lo referente tanto a la protección de datos de las personas, como el derecho a la intimidad personal y familiar, y a la inviolabilidad de la correspondencia tanto física como virtual, circunstancia que no se cumple y es vulnerada y afectada a través de este tipo de publicidad no solicitada.

En la presente temática, se piensa que es necesario realizar un cambio en los problemas que se suscitan con el avance tecnológico, esto es, el limitar la propaganda y publicidad no deseada ni solicitada a través de mensajes ya sea por la utilización del correo electrónico, páginas web o mensajes a celulares, lo cual resulta un fraude para mi punto de vista que no está siendo sancionado en nuestro país.

La presente investigación gira en torno a la existencia de un problema jurídico y social trascendente y actual, de una importancia que alcanza una trascendencia en el estudio jurídico contemporáneo. Además de ello debo manifestar que cuento con la bibliografía necesaria que me permitirá realizar una fundamentación importante al tema planteado.

La presente investigación además de cumplir con los requisitos previstos en el Reglamento de Régimen Académico de la Universidad Nacional de Loja; y, de constituir un requisito previo a la obtención de mi título de Abogada; constituye por sí sólo en un problema jurídico de trascendencia económica, social; y, política en nuestro medio que marca su importancia jurídica para su análisis, estudio, y su consecuente transformación para garantizar los

derechos de las personas.

Esta circunstancia es la que configura la problemática; pues considero que es necesario que el procedimiento coactivo en materia tributaria debe cumplir con los principios determinados en la Constitución de la República; además de que tratándose el título de crédito tributario un documento que exige el cumplimiento de una obligación pendiente cuya falta de pago perjudica al Estado; deben gozar dichos instrumentos de la calificación de títulos preferentes, ante otros documentos que exijan del mismo obligado el cumplimiento de obligaciones pendientes.

Identificado el problema, objeto de estudio, luego de efectuar la investigación debidamente planificada, redacté el presente Informe Final el cual en su estructura sigue los lineamientos establecidos por el Reglamento de Régimen Académico de la Universidad Nacional de Loja; y, que me ha permitido contar con una información doctrinaria y jurídica establecida dentro de tres marcos importantes como son el Marco Conceptual, a través del cual establezco en orden de tratamiento los conceptos de cada una de las variables utilizadas en la elaboración de la presente investigación; el Marco Doctrinario a través del cual me permito incluir en este trabajo el análisis; y, los criterios de diferentes autores que han realizado diversos estudios en relación a la problemática; y, el Marco Jurídico en el que utilizando la normativa legal vigente, abordo los temas, materia del trabajo de investigación.

Avanzando con la estructura del presente trabajo, encontrarán el punto de

Materiales y Métodos, en donde explico la forma en que se ha utilizado cada uno de los métodos, las técnicas de investigación; y, los materiales que se han empleado en el desarrollo de la investigación de campo, en donde se realiza un análisis y presentación de los resultados de las treinta encuestas aplicadas, dentro de este trabajo las mismas que se encuentran establecidas por el procesamiento de datos que fueron aplicados a Abogados en libre ejercicio quienes con conocimiento de causa nos brindan su posición respecto a este tema.

Posteriormente en el punto denominado Discusión verifiqué los objetivos, contrasté la hipótesis y expreso los fundamentos jurídicos del proyecto de reforma.

En las Conclusiones se presenta una síntesis de los resultados obtenidos después de la investigación realizada. Además establezco algunas Recomendaciones a más de incluir el Proyecto de Reforma como el punto principal a plantear.

Finalmente la Bibliografía cuenta con una descripción en una lista de todas las obras consultadas que me ha servido para poder culminar mi trabajo de tesis. En los Anexos incluyo los modelos de encuesta y entrevista realizados a profesionales del derecho, a los diferentes grupos relacionados con la materia además del Proyecto de investigación; y, el Índice.

4. REVISIÓN DE LITERATURA

4.1. MARCO CONCEPTUAL

4.1.1. Comercio Electrónico.- Para Renato Jijena Leiva "el comercio electrónico es: el intercambio Electrónico o Telemático de información entre personas que da lugar a una relación comercial, consistente en la entrega en línea de bienes intangibles o en un pedido electrónico de bienes tangibles"[1].

Para otros autores el concepto de comercio electrónico puede ser visto de diferentes maneras, una restrictiva: "el pago electrónico dentro de Internet, de un bien adquirido por Internet", una amplia, que indica que: "el comercio electrónico, es el intercambio de bienes y servicios por medios electrónicos, siendo su pago posible también por dicho medio", pasando por la propuesta por la WTO (Organización Mundial del Comercio): "the distribution, marketing, sale or delivery of goods and services by electronic means."[2].

Para la OCDE, "el comercio Electrónico o Telemático se refiere a transacciones comerciales, envolviendo organizaciones e individuos, basadas en el proceso y transmisión de datos digitalizados, incluyendo texto, sonido e imágenes visuales que son transmitidas por redes abiertas como Internet o redes cerradas"[3].

Otra definición indica que el comercio Electrónico o Telemático es: "la capacidad para compradores y vendedores de conducir negocios y/o

[1] JIJENA LEIVA Renato, Chile: Comercio Electrónico y Derecho, La problemática jurídica del Comercio Electrónico. Artículo Publicado en Internet
[2] IRIARTE AHON Erick, Comercio Electrónico en América Latina y el Caribe Perspectivas y realidades. Artículo Publicado en Internet

intercambiar informaciones en tiempo real en interacciones humanas"[4]

La OMC (Organización Mundial de Comercio) define al Comercio Electrónico o Telemático como: "La distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos"[5]

En la Ley de Comercio Electrónico de nuestro país en su glosario de términos encontramos la definición de comercio electrónico: es toda transacción, comercial realizada en parte o en su totalidad a través de redes electrónicas de información.

En definitiva diremos que Comercio Electrónico o Telemático es: Es toda transacción telemática de información realizada mediante el uso de mensajes de datos, de carácter gratuito u oneroso entre dos o más personas que da como resultado una relación comercial, civil, financiera, bursátil o de cualquier otra índole consistente en la adquisición de bienes tangibles, intangibles, o la prestación de un servicio.

4.1.2. MENSAJES DE DATOS.- "Se entenderá como la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax"[6]

"Es importante comenzar destacando que el mensaje de datos también llamado documento electrónico, tanto desde el punto de vista tecnológico,

[4] OCDE. Policy Brief Electronic Commerce, No. 1 - 1997
[5] Chakraborty, Simanta, Sapient Corp.| 18.11.1998
[6] JIJENA LEIVA Renato, Chile: Comercio Electrónico y Derecho, La problemática jurídica del Comercio Electrónico. Artículo Publicado en Internet

como desde el punto de vista jurídico, implica la emisión de información la cual puede ser de ciencia, de conocimiento o de voluntad."[7]

Los mensajes de datos son un concepto propio de las firmas digitales en los que se entiende como tal a cualquier tipo de mensaje enviado o recibido por medio electrónico u óptico. Por lo general se entiende a comunicaciones efectuadas mediante correo electrónico; sin embargo, también se extiende a otras comunicaciones como el telegrama, el telex o el telefax. Fuera de su definición legal, para los efectos prácticos, el *mensaje de datos* es un concepto final que agrupa a todos los componentes del *documento electrónico*, ya que al referirnos al mensaje de datos nos referimos a varios elementos. Un mensaje de datos, por lo tanto, puede estar compuesto por datos en particular, (que a su vez se subdividen en bit y bytes), los mismos se organizan en segmentos, que a su vez se estructuran en un todo comprensible denominado *texto*, siendo éste el elemento clásico que contiene toda la información de un documento en soporte papel, (tal como la hora, fecha, nombre de empresa, etc.), y finalmente, el anexo de un dato identificador o firma digital.

[7] http://www.entorno-empresarial.com/articulo/2151/el-mensaje-de-datos

4.2. MARCO DOCTRINARIO

4.2.1. Breve reseña Histórica del aparecimiento y uso de las nuevas tecnologías y el Internet.

Hoy en día es común ver como cada vez estamos siendo más dependientes de las computadoras como herramienta indispensable. Ya no es extraño ver que una gran parte de la población tiene acceso a este tipo de dispositivos informáticos, ni tampoco es el hecho de que puedan tener acceso a la red de redes, que es el Internet. También, muchas de las actividades que solían hacerse manualmente, ahora pueden hacerse a través de medios informáticos, lo cual es una gran ventaja, pues se ahorra tiempo, y dinero la mayoría de las veces. Pero así como se puede aprovechar la tecnología para cosas buenas, también se pueden aprovechar para cometer delitos. Por lo tanto, hoy en día es común ver que se cometen una gran cantidad de delitos en los que se ve involucrado algún sistema de cómputo ya sea como medio, o fin.

Muchos países, en especial, los países desarrollados, ya cuentan con una Ley sobre Delitos Informáticos, otros, como el caso de nuestro país, hacen un apartado en su Constitución para contemplar también los delitos informáticos, mientras que hay países que ni siquiera se menciona sobre delitos informáticos en su ley.

Es importante tener una clara idea de lo que es y no es un delito informático. Prácticamente podemos clasificar los delitos informáticos dentro de dos áreas, donde la primera son Delitos Informáticos de naturaleza, y la otra que contempla aquellos delitos que, aunque no sean delitos informáticos, se consideran como tales por hacer uso de una computadora como medio.

Entre los delitos informáticos más comunes, encontramos: sabotajes, fraudes, estafas, pesca de contraseñas, juegos de azar, lavado de dinero, copia ilegal de software, espionaje, infracción del copyright en bases de datos, uso ilegítimo de Sistemas Informáticos ajenos, accesos no autorizados, interceptación de correo electrónico, pornografía infantil, falsificación, etc. Además de otras actividades graves como: terrorismo, narcotráfico, espionaje, actos parasitarios, tráfico de armas, proselitismo de sectas, etc.

A partir de la década de los sesenta, la humanidad descubrió las ventajas que trae consigo la tecnología.

El ser humano poco a poco, logró automatizar muchas de sus actividades. Se ahorra tiempo y recursos con el empleo de lo que se denomina "inteligencia artificial". Es difícil imaginar alguna actividad humana en la que no intervengan máquinas dotadas de gran poder de resolución.

La informática, entendiéndola como el uso de computadoras y sistemas que ayudan a mejorar las condiciones de vida del hombre, la encontramos en todos los campos: en la medicina, en las finanzas, en el Derecho, en la industria, entre otras.

En la actualidad con la creación de la denominada "autopista de la información", el INTERNET, las posibilidades de comunicación e investigación se han acrecentado, se tiene acceso a un ilimitado número de fuentes de consulta y entretenimiento.

El problema radica en que, la conducta humana parece ser que está inclinada

al delito, a conseguir satisfacción a sus deseos a toda costa. Con el desarrollo de la informática, aparece también lo que se denomina como: DELITO INFORMATICO.

De la misma manera que muchas personas se han dedicado a desarrollar sistemas de computación para solucionar problemas de la sociedad, otras tratan de utilizar la tecnología, y en el caso que nos ocupa, las computadoras y sistemas, para el cumplimiento de actividades ilícitas.

De la misma forma como se encuentran cosas positivas en el INTERNET, encontramos cosas negativas, lo cual nos lleva a pensar que el mal no está en la tecnología sino en las personas que las usan, a modo de ejemplificación diremos que la red de comunicación electrónica digital, se la ha utilizado por pederastas para estimular la prostitución infantil, del mismo modo grupos políticos racistas neo nazis lo han usado para difundir su nefasta ideología, se cree, inclusive, que el INTERNET es una vía de comunicación y negocios entre narcotraficantes y contrabandistas de armas, etc.

4.2.2. El Fenómeno de la Delincuencia Informática

El aspecto más importante de la informática radica en que la **información** ha pasado ha convertirse en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después[8].

[8] MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999

Como señala Camacho Losa, "En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia[9]." Entonces el autor se pregunta ¿y por qué la informática habría de ser diferente?

Existe un consenso general entre los diversos estudiosos de la materia, en considerar que el nacimiento de esta clase de criminalidad se encuentra íntimamente asociada al desarrollo tecnológico informático. Las computadoras han sido utilizadas para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato. Los primeros casos fueron reportados en 1958.

Para el profesor Manfred Mohrenschlager "este fenómeno ha obligado al surgimiento de medidas legislativo penales en los Estados Industriales donde hay conciencia de que en los últimos años, ha estado presente el fenómeno delictivo informático"[10].

En nuestro país, el fenómeno de la criminalidad informática o de los llamados delitos informáticos, no han alcanzado todavía una importancia mayor, esto por cuanto no se conoce en nuestro entorno mucho sobre esta clase de infracciones a pesar del efecto de aldea global que estamos viviendo, y la razón de que esta nueva forma de lesión a bienes jurídicos tutelados no sea tomada en cuenta, es porque se ha perdido por parte de la legislación penal nacional la conexión entre ésta y la realidad social actual.

[9] CAMACHO LOSA Luis, El Delito Informático, Madrid, España, 1987.
[10] MOHRENSCHLAGER, Manfred. El Nuevo Derecho Penal informático en Alemania" (Págs. 99 a 143).

4.2.2.1. Delincuencia informática y Abuso Informático

La define Gómez Perals como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

La misma definición aporta Correa incidiendo en la Recomendación (89) 9. Del Comité de Ministros del Consejo de Europa considerando que la delincuencia informática suele tener carácter transfronterizo que exige una respuesta adecuada y rápida y, por tanto, es necesario llevar a cabo una armonización más intensa de la legislación y de la práctica entre todos los países respecto a la delincuencia relacionada con el computador.

4.2.3. Criminalidad informática

Baón Ramírez define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevadas a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

Tiedemann[11] considera que con la expresión "criminalidad mediante computadoras", se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento

[11] TIEDEMANN, Klaus, Poder informático y delito, Barcelona, España. 1985.

de datos.

Como el mismo autor señala, el concepto abarca el problema de la amenaza a la esfera privada del ciudadano, y por otra parte, se refiere además a los daños patrimoniales producidos por el abuso de datos procesados automáticamente.

Para Carlos Sarzana, en su obra Criminalità e tecnología, los crímenes por computadora comprenden cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo.

4.2.4. Sujetos del Delito Informático

En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo[12].

4.2.4.1. Sujeto Activo.- De acuerdo al profesor chileno Mario

[12] HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur.

Garrido Montt[13], se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal.

Las personas que cometen los "**Delitos Informáticos**" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que "desvía fondos" de las cuentas de sus clientes.

Tiedemann, frente a esta definición nos dice "De manera creciente, en la nueva literatura angloamericana sobre estos temas se emplea el término **"hecho penal profesional"** (Occupational Crime). Con esta referencia al papel profesional y a la actividad económica, la caracterización del delito económico se fundamenta ahora menos en la respetabilidad del autor y su

---

[13] GARRIDO MONTT, MARIO. Nociones Fundamentales de la Teoría del Delito Edit. Jurídica de Chile, 1992. Citado por Jijena Leiva Renato, Los Delitos Informáticos y la Protección Penal a la Intimidad, Editorial Jurídica de Chile, 1993

pertenencia a la capa social alta y más en la peculiaridad del acto (modus operandi) y en el objetivo del comportamiento"[14].

A este respecto Marcelo Huerta y Claudio Líbano dicen que "en lo relativo a tratarse de "Ocupacional Crimes", es cierto que muchos de los delitos se cometen desde dentro del sistema por personas que habitualmente lo operan y que tienen autorizado los accesos (**Insiders**). Sin embargo, las tendencias modernas apuntan hacia el campo de la teleinformática a través del mal uso del ciberespacio y las supercarreteras de la información o redes de telecomunicaciones. Es decir, cada día gana más terreno el delito informático a distancia. (**Outsiders**)."[15]

Es difícil elaborar estadísticas sobre ambos tipos de delitos (delitos de cuello blanco y delitos informáticos). La "**cifra negra**" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables". Esto en el caso de los delitos informáticos tiene relación con lo que se ha dado a llamar el síndrome de "**Robin Hood**" es decir a "la creencia en cierto modo patológica de que mientras que robar a una persona física que tiene sus problemas y necesidades materiales como todo hijo de

[14] TIEDEMANN, Klaus, Poder Económico y Delito
[15] HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur.

vecino es un hecho inmoral e imperdonable, robar a una institución como la banca que gana decenas de miles de millones al año es casi un acto social que contribuye a una más justa distribución de la riqueza"[16].

Como sostiene Gutiérrez Francés, "con carácter general, la delincuencia mediante computadoras se inscribe dentro de las formas de criminalidad de "Cuello Blanco", propias de la delincuencia económica, por lo cual desde el punto de vista criminológico, presentan las mismas peculiaridades que ésta, con las notas específicas que aporta lo informático"[17].

Por mi parte, considero que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, por tanto diremos que la cualificación del sujeto activo no es un elemento determinante en la delincuencia informática. Sólo algunos delitos, como los cometidos por los hackers propiamente dichos, podrán considerarse como realizados por un sujeto altamente calificado. Los más, no requieren, en cuanto al sujeto, calificación, ya que pueden cometerse por personas que recién se inician en la informática o por niños que están aprendiendo individualmente en sus hogares.

A este respecto el jurista mexicano Jorge Lara Rivera, en un artículo publicado en Internet[18] nos dice que "Tradicionalmente se ha considerado que este tipo de delitos se encuadra dentro de los llamados "delitos de cuello blanco" debido a que se requiere que el sujeto activo tenga un conocimiento

16 CAMACHO LOSA, Luis, El Delito Informático.
17 GUTIÉRREZ FRANCÉS, María Luz, Fraude Informático y estafa.
18 LARA RIVERA, Jorge, Los Delitos Informáticos. www.jusrismática.com.

especializado en informática. Ahora bien, no podemos negar que la especialización informática facilita a los sujetos a incidir criminalmente por medio de las computadoras. Sin embargo, el mundo de la computación se va convirtiendo paulatinamente en un área común y corriente, gracias a la facilidad con la que los modernos sistemas y programas pueden ser controlados. Dentro de poco tiempo la operación de un sistema electrónico será tan fácil como manejar una televisión, por ejemplo. De esta manera, se puede ubicar como sujeto activo de un delito cibernético a un lego en la materia o a un empleado de un área no informática que tenga un mínimo conocimiento de computación. Por no hablar del problema que se plantea con los llamados "niños genio" que son capaces no sólo de dominar sistemas electrónicos básicos, sino que pueden incluso intervenir exitosamente en operaciones de alto grado de dificultad técnica, acarreando más problemas al tambaleante concepto de la impunidad para el caso de que algunos de estos menores logre cometer estragos importantes a través de los medios computacionales que maneje".

4.2.5. Sujeto Pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.

En primer término tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones creditícias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a

otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los “delitos informáticos”, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, “ha sido imposible conocer la verdadera magnitud de los “delitos informáticos”, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables” y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; La falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada “cifra oculta” o “cifra negra”.

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de

manipulación, así como sus formas de encubrimiento.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas, además de que en

algunos países como el nuestro no existe legislación alguna sobre esta clase de conductas ilícitas lo que empeora más la situación de las víctimas de estas conductas ilícitas.

4.2.6. Bien Jurídico Protegido

El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir –ya que constituye la razón de ser del delito– y no suele estar expresamente señalado en los tipos penales.

Dentro de los delitos informáticos, podemos decir que la tendencia es que la protección a los bienes jurídicos, se le haga desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como regla general que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

De otro lado otra vertiente doctrinaria supone que la emergente Sociedad de la Información hace totalmente necesaria la incorporación de valores inmateriales y de la **información** misma como **bienes jurídicos de protección,** esto tomando en cuenta las diferencias existentes por ejemplo entre la propiedad tangible y la intangible. Esto por cuanto la información no puede a criterio de Pablo Palazzi ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, si bien dichos bienes

tiene un valor intrínseco compartido, que es su valoración económica, es por tanto que ella la información y otros intangibles son objetos de propiedad, la cual esta constitucionalmente protegida.

En fin la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de "dañosidad" o "lesividad". Así, una conducta sólo puede conminarse con una pena cuando resulta del todo incompatible con los presupuestos de una vida en común pacífica, libre y materialmente asegurada. Así inspira tanto a la criminalización como a descriminalización de conductas. Su origen directo es la teoría del contrato social, y su máxima expresión se encuentra en la obra de BECCARIA "Los Delitos y las Penas" (1738-1794). Se define como un bien vital, "bona vitae", estado social valioso, perteneciente a la comunidad o al individuo, que por su significación, es garantizada, a través del poder punitivo del Estado, a todos en igual forma.

En conclusión podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

- El patrimonio, en el caso de la amplia gama de fraudes informáticos y

las manipulaciones de datos que da a lugar.

- La reserva, la intimidad y confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.
- La seguridad o fiabilidad del tráfico Jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.
- El derecho de propiedad, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático.

Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

Para los autores chilenos Claudio Magliona y Macarena López, sin embargo los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo"[19]. En conclusión no se afecta un solo bien jurídico, sino una diversidad de ellos.

Por tanto podemos decir que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino que la multiplicidad de conductas que la

[19] REYES ECHANDÍA, Alfonso, La Tipicidad, Universidad de Externado de Colombia, 1981.

componen afectan a una diversidad de ellos que ponen en relieve intereses colectivos, en tal sentido de María Luz Gutiérrez Francés, respecto de la figura del fraude informático nos dice que: "las conductas de fraude informático presentan indudablemente un carácter pluriofensivo. En cada una de sus modalidades se produce una doble afección: la de un interés económico (ya sea micro o macrosocial), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macrosocial vinculado al funcionamiento de los sistemas informáticos"[20].

Por tanto diremos que el nacimiento de esta nueva tecnología, está proporcionando a nuevos elementos para atentar contra bienes ya existentes (intimidad, seguridad nacional, patrimonio, etc.), sin embargo han ido adquiriendo importancia nuevos bienes, como sería la calidad, pureza e idoneidad de la información en cuanto tal y de los productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa[21]. En tal razón considero que este tipo de conductas criminales son de carácter netamente pluriofensivo.

Un ejemplo que puede aclarar esta situación, es el de un hacker que ingresa a un sistema informático con el fin de vulnerar la seguridad éste y averiguar la información que más pueda sobre una determinada persona, esto en primer lugar podríamos decir que el bien jurídico lesionado o atacado es el derecho a la intimidad que posee esa persona al ver que su información personal es

[20] GUTIÉRREZ FRANCÉS, María Luz, Fraude Informático y estafa.
[21] MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999

vista por un tercero extraño que sin autorización ha vulnerado el sistema informático donde dicha información está contenida. Pero detrás de ese bien jurídico encontramos otro un bien colectivo que conlleva a un ataque a la confianza en el funcionamiento de los sistemas informáticos. Es decir, de intereses socialmente valiosos que se ven afectados por estas nuevas figuras, y que no solo importan la afección de bienes jurídicos clásicos.

4.2.7. Tipos de Delitos informáticos

Existen muchos tipos de delitos informáticos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es inimaginable, a decir de Camacho Losa, el único límite existente viene dado por la conjugación de tres factores: la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas, por tal razón y siguiendo la clasificación dada por el estadounidense Don B. Parker más la lista mínima de ilícitos informáticos señalados por las Naciones Unidas, he querido lograr una clasificación que desde el punto de vista objetivo sea lo más didáctica posible al momento de tratar esta clase de conductas delictivas, por lo expuesto anteriormente y sin pretender agotar la multiplicidad de conductas que componen a esta clase de delincuencia y como señala Gutiérrez Francés, es probable que al escribir estas líneas ya hayan quedado sobrepasada las listas de modalidades conocidas o imaginables, que ponemos a consideración del lector en forma breve en que consiste cada una de estas conductas delictivas:

4.2.8. Los fraudes

Data diddling.- Conocidos también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Troya Horses.- Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Salami Technique/Rounching Down.- Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina “técnica del salchichón” en la que “rodajas muy finas” apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas

instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

Falsificaciones informáticas: Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada. **Como instrumentos:** Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

Manipulación de los datos de salida.- Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Pishing.- Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener

información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las victimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aun peor. En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar.

En estos momentos también existe una nueva modalidad de Pishing que es el llamado Spear Pishing o Pishing segmentado, que funciona como indica el gráfico 1, el cual ataca a grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior.

4.2.9. El sabotaje informático.

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Bombas lógicas (Logic Bombs), es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos,

las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

Gusanos. Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita. (Gráfico 2)

Virus informáticos y malware, son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos.

Un virus puede ingresar en un sistema por conducto de una pieza legítima de

soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. Han sido definidos como "pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autorreporducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar"[22].

El malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y la debilidades de los sistemas desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos.

Ciberterrorismo: Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

Ataques de denegación de Servicio: Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima,

[22] GUIBOURG Ricardo A., ALENDE Jorge O., CAMPANELLA Elena M., Manual de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires, Argentina.

hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

4.2.10. El espionaje informático y el robo o hurto de software:

Fuga de datos (Data Leakage), también conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Loza, "la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera"[23].

La forma más sencilla de proteger la información confidencial es la criptografía.

Reproducción no autorizada de programas informáticos de protección legal. Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al

[23] CAMACHO LOSA, Luis, El Delito Informático, Madrid, España, 1987.

respecto, considero, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

4.2.11. El robo de servicios:

Hurto del tiempo del computador. Consiste en el hurto de el tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no esta autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

Apropiación de informaciones residuales (Scavenging), es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. To scavenge, se traduce en recoger basura. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

Parasitismo informático (Piggybacking) y Suplantación de personalidad

(Impersonation), figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización o empresa determinada.

4.2.12. El acceso no autorizado a servicios informáticos:

Las puertas falsas (Trap Doors), consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

La llave maestra (Superzapping), es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.

Su nombre deriva de un programa utilitario llamado superzap, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador.

Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación

Pinchado de líneas (Wiretapping), consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

Como se señaló anteriormente el método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía que consiste en la aplicación de claves que codifican la información, transformándola en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y por aplicación de las mismas claves, la información se recompone hasta quedar exactamente igual a la que se envió en origen.

Piratas informáticos o hackers. El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

4.3. MARCO JURÍDICO

4.3.1. TRATADOS Y CONVENIOS INTERNACIONALES RESPECTO DE LA PREVENCION DEL DELITO INFORMÁTICO Y LA PROTECCIÓN CONTRA MENSAJES DE DATOS DE COMUNICACIÓN NO SOLICITADOS.

4.3.1.1. Organización de Estados Americanos.-

La Internet y las redes y tecnologías relacionadas se han convertido en instrumentos indispensables para los Estados Miembros de la OEA. La Internet ha impulsado un gran crecimiento en la economía mundial y ha aumentado la eficacia, productividad y creatividad en todo el Hemisferio. Individuos, empresas y gobiernos cada vez utilizan más las redes de información que integran la Internet para hacer negocios; organizar y planificar actividades personales, empresariales y gubernamentales; transmitir comunicaciones; y realizar investigaciones. Asimismo, en la Tercera Cumbre de las Américas, en la ciudad de Québec, Canadá, en 2001, nuestros líderes se comprometieron a seguir aumento la conectividad en las Américas.

Lamentablemente, la Internet también ha generado nuevas amenazas que ponen en peligro a toda la comunidad mundial de usuarios de Internet. La información que transita por Internet puede ser malversada y manipulada para invadir la privacidad de los usuarios y defraudar a los negocios. La destrucción de los datos que residen en las computadoras conectadas por Internet puede obstaculizar las funciones del gobierno e interrumpir el servicio público de telecomunicaciones y otras infraestructuras críticas.

Estas amenazas a nuestros ciudadanos, economías y servicios esenciales, tales como las redes de electricidad, aeropuertos o suministro de agua, no pueden ser abordadas por un solo gobierno ni tampoco pueden combatirse utilizando una sola disciplina o práctica. Como reconoce la Asamblea General en la resolución AG/RES. 1939 (XXXIII-O/03) (**Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética**), es necesario desarrollar una estrategia integral para la protección de las infraestructuras de información que adopte un enfoque integral, internacional y multidisciplinario. La OEA está comprometida con el desarrollo e implementación de esta estrategia de seguridad cibernética y en respaldo a esto, celebró una Conferencia sobre Seguridad Cibernética (Buenos Aires, Argentina, del 28 al 29 de julio de 2003) que demostró la gravedad de las amenazas a la seguridad cibernética para la seguridad de los sistemas de información esenciales, las infraestructuras esenciales y las economías en todo el mundo, y que una acción eficaz para abordar este problema debe contar con la cooperación intersectorial y la coordinación entre una amplia gama de entidades gubernamentales y no gubernamentales.

La Estrategia Interamericana Integral de Seguridad Cibernética se basa en los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL), y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA). La Estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con

respecto a la seguridad a fin de crear una cultura de seguridad cibernética.

La Estrategia también reconoce que un marco eficaz para la protección de las redes y sistemas de información que integran la Internet y para responder a incidentes y recuperarse de los mismos dependerá en igual medida de que:

- Se proporcione información a los usuarios y operadores para ayudarles a asegurar sus computadoras y redes contra amenazas y vulnerabilidades, y a responder ante incidentes y a recuperarse de los mismos;
- Se fomenten asociaciones públicas y privadas con el objetivo de incrementar la educación y la concientización, y se trabaje con el sector privado –el cual posee y opera la mayoría de las infraestructuras de información de las que dependen las naciones—para asegurar esas infraestructuras;
- Se identifiquen y evalúen normas técnicas y prácticas óptimas para asegurar la seguridad de la información transmitida por Internet y otras redes de comunicaciones, y se promueva la adopción de las mismas; y
- Se promueva la adopción de políticas y legislación sobre delito cibernético que protejan a los usuarios de Internet y prevengan y disuadan el uso indebido e ilícito de computadoras y redes.

4.3.2. La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional

El crimen organizado trata principalmente de la búsqueda de ganancias y se

lo puede entender, en términos Clausewitzianos[24] como una continuación de los negocios por medios delictivos esto a decir de **Phil Williams** Profesor de Estudios de Seguridad Internacional, Universidad de Pittsbugh. Por consiguiente, igual que las compañías de ladrillos y argamasa trasladan sus empresas al World Wide Web en procura de nuevas oportunidades de ganancias, las empresas delictivas están haciendo lo mismo. Las organizaciones criminales no son los únicos participantes en los mercados ilícitos, pero muchas veces son los más importantes, no sólo debido a la "competitividad" adicional que provee la amenaza de la violencia organizada. Además, las organizaciones criminales tienden a ser excepcionalmente hábiles en identificar y aprovechar oportunidades para nuevas empresas y actividades ilegales. En este contexto, la Internet y el crecimiento continuo del comercio electrónico ofrecen nuevas y enormes perspectivas de ganancias ilícitas[25].

Es por tanto que la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, que entró en vigor en septiembre de 2003, es el principal instrumento internacional en la lucha contra la delincuencia organizada. La Convención tiene 147 Estados Signatarios y 100 Estados Parte y de la cual el Ecuador es parte, en dicha convención se pone de manifiesto las reglas básicas sobre la prosecución de Delincuencia Organizada Transnacional, dichas reglas hacen especial mención de los

---

[24] Se refiere al filósofo alemán KARL VON CLAUSEWITZ, reconocido por la máxima "*La guerra es una continuación de la política por otros medios*"

[25] PHIL WILLIAMS, Crimen Organizado y Cibernético, sinergias, tendencias y respuestas. Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon. http://www.pitt.edu/~rcss/toc.html

delitos relacionados con la legitimación de activos y los de corrupción. También se mencionan a los llamados “delitos graves” que son de acuerdo con el Art. 2 toda “conducta que constituya un delito punible con una privación de libertad máxima de al menos cuatro años o con una pena más grave”. En el caso de las llamadas infracciones informáticas todas ellas son delitos graves de acuerdo a la definición de la Convención, en tal razón se encuadran en su ámbito de aplicación de la convención de conformidad al Art. 3, siempre que dichos delitos sean de carácter transnacional y entrañen la participación de un grupo delictivo organizado.

De igual forma se debe tomar en cuenta que la Convención da la posibilidad de conseguir capacitación y asistencia de parte de los Estados signatarios en la prevención e investigación de esta clase de delitos e insta a contar con programas de capacitación y entrenamiento a las personas responsables del cumplimiento de la ley como Jueces, Fiscales y Policías. También insiste en el uso de Técnicas Especiales de Investigación como la vigilancia electrónica.

4.3.3. NORMAS CONSTITUCIONALES Y POLITICAS ESTATALES QUE SUSTENTAN LA PROTECCION CONTRA DELITOS INFORMATICOS, INCLUIDO EL ENVIO DE MENSAJE DE DATOS.

Dentro de este esfuerzo que se ha venido dando, tanto en el ámbito interno de cada país como a nivel internacional, para perseguir los delitos informáticos nos encontramos ante el caso de Ecuador que en los últimos años se ha comenzado a legislar sobre este tema.

Dicho esfuerzo se hace más evidente en nuestro país con la aprobación de la Constitución de la República del Ecuador del 2008, que establece en las siguientes disposiciones legales lo siguiente:

Art. 16 establece lo siguiente: "Derecho a la comunicación.- Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.

2. El acceso universal a las tecnologías de información y comunicación.

3. La creación de medios de comunicación social, y al acceso en igual de condiciones al uso de las frecuencias del espectro radioelectrónico para la gestión de estaciones de radio y televisión pública privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.

4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.

5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación"[26]

Art. 17 "EI Estado fomentará la pluralidad y la diversidad en la Comunicación y al efecto:

1. Garantizará la asignación, a través de métodos transparentes y en igualdad

[26] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Art. 16

de condiciones, de las frecuencias del espectro radioeléctrico, para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, así como el acceso a bandas libres para la explotación de redes inalámbricas, y precautelará que en su utilización prevalezca el interés colectivo.

2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada.

3. No permitirá el oligopolio o monopolio, directo ni indirecto, de la propiedad de los medios de comunicación y del uso de las frecuencias."[27]

Art. 18.- De la Constitución de la República "Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad

[27] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Art. 17

pública negará la información."[28]

El Art 66 en sus numerales 19 y 21 establece: "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión, que incluye acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley.

Numeral 21.- El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación"[29]

Art.385.- Ciencia, tecnología, innovación y saberes ancestrales.- "El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.

2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción

[28]CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Art. 18
[29] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Art. 66, num 19 y 21

nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir."[30]

Art. 386.- "El sistema comprenderá programas, políticas, recursos, acciones, e incorporará a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y particulares, empresas públicas y privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación y aquellas ligadas a los saberes ancestrales.

El Estado, a través del organismo competente, coordinará el sistema, establecerá los objetivos y políticas, de conformidad con el Plan Nacional de Desarrollo, con la participación de los actores que lo conforman."[31]

Art. 387.- "Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.

2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, al sumak kawsay.

3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.

[30] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Art. 385
[31] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Art. 387

4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.

5. Reconocer la condición de investigador de acuerdo con la Ley."[32]

Art. 388.- "El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento.

Un porcentaje de estos recursos se destinará a financiar proyectos mediante fondos concursables. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo."[33]

En el año 2002 se aprobó en nuestro país la LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJE DE DATOS, pero como se darán cuenta la presente ley según su objetivo tipificado en el Art. 1 es el siguiente: "Esta ley regula los mensajes de datos, las firmas electrónicas, los servicios de certificación, la contratación electrónica y telemática, la presentación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas."[34]

Como nos podemos dar cuenta, esta ley no tipifica los delitos cometidos a

[32] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Art. 387
[33] CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Art. 388
[34] LEY DE COMERCIO ELECTRÓNICO, ART. 1

través de las redes informáticas, peor aún el espionaje electrónico al que estamos expuestos todas las personas como también el Estado. Nuestra legislación penal los tipifica a esta clase de delitos de una manera muy general, y las víctimas de esta clase de delitos so se encuentran legalmente protegidos y en muchas ocasiones esta clase de delitos se quedan en la impunidad.

Como podemos ver nuestro Código Penal hace un enfoque generalizado de los delitos cometidos a través de las redes informáticas, pero en cuanto a los delitos cometidos en contra de una persona o instituciones, pero no en contra de un Estado a través de redes electrónicas, si se diera deberíamos atenernos a lo dispuesto en el Art. 5 del Código Penal, hace mención sobre la territorialidad de la ley, ya que; esta será aplicada dentro del territorio ecuatoriano y de ahí la necesidad de que los estados cooperen con el afán de dar un trámite legal adecuado a los delitos informáticos, como también el espionaje electrónico.

4.3.4. El Delito Informático y su realidad procesal en las normas constitucionales y legales ecuatorianas.

Desde que en 1999 en el Ecuador se puso en el tapete de la discusión el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, desde ese tiempo se puso de moda el tema, se realizaron cursos, seminarios, encuentros. También se conformó comisiones para la discusión de la Ley y para que formulen observaciones a la misma por parte de los organismos directamente interesados en el tema como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, que ven el

Comercio Electrónico o Telemático una buena oportunidad de hacer negocios y de paso hacer que nuestro país entre en el boom de la llamada Nueva Economía.

Cuando la ley se presentó en un principio, tenía una serie de falencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal de dicha ley, ya que las infracciones a la misma es decir los llamados Delitos Informáticos, como se los conoce, se sancionarían de conformidad a lo dispuesto en nuestro Código Penal, situación como comprenderán era un tanto forzada, esto si tomamos en cuenta los 65 años de dicho Código, en resumen los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática por tanto les hacía inútiles por decirlo menos, para dar seguridad al Comercio Electrónico o Telemático ante el posible asedio de la criminalidad informática.

Por fin en abril del 2002 y luego de largas discusiones los honorables diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos.

Ahora bien el problema que se advierte por parte de las instituciones llamadas a perseguir las llamadas infracciones informáticas es la falta de preparación en el orden técnico tanto del Ministerio Público como de la Policía Judicial, esto en razón de la falta por un lado de la infraestructura necesaria, como centros de vigilancia computarizada, las modernas

herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de los llamados Delitos Informáticos, de igual manera falta la suficiente formación tanto de los Fiscales que dirigirán la investigación como del cuerpo policial que lo auxiliara en dicha tarea, dado que no existe hasta ahora en nuestra policía una Unidad Especializada, como existe en otros países como en Estados Unidos donde el FBI cuenta con el Computer Crime Unit, o en España la Guardia Civil cuenta con un departamento especializado en esta clase de infracciones. De otro lado también por parte de la Función Judicial falta la suficiente preparación por parte de Jueces y Magistrados en tratándose de estos temas, ya que en algunas ocasiones por no decirlo en la mayoría de los casos los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por su estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin.

Por tanto es esencial que se formen unidades Investigativas tanto policiales como del Ministerio público especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. Lo cual es posible aplicando la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos.

La cooperación multilateral de los grupos especiales multinacionales pueden

resultar ser particularmente útiles - y ya hay casos en que la cooperación internacional ha sido muy efectiva. De hecho, la cooperación puede engendrar emulación y éxitos adicionales.

De otro lado en los últimos tiempos la masificación de virus informáticos globales, la difusión de la pornografía infantil e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos y sin fronteras que presentan una realidad difícil de controlar. Con el avance de la tecnología digital en los últimos años, ha surgido una nueva generación de delincuentes que expone a los gobiernos, las empresas y los individuos a estos peligros.

Es por tanto como manifiesta **Phil Williams** Profesor de Estudios de Seguridad Internacional, Universidad de Pittsbugh[35], Es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la Delincuencia Informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delitos transnacionales.

Es por estas razones que el Ministerio Público tiene la obligación Jurídica en cumplimiento de su mandato constitucional de poseer un cuerpo especializado para combatir esta clase de criminalidad a fin de precautelar los derechos de las víctimas y llevar a los responsables a juicio, terminando

[35] WILLIAMS PHIL, Crimen Organizado y Cibernético, sinergias, tendencias y respuestas. Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon. http://www.pitt.edu/~rcss/toc.html

así con la cifra negra de esta clase de infracciones, ya que en la actualidad esta clase de conductas ilícitas no son tratadas en debida forma por los órganos llamados a su persecución e investigación, así por ejemplo un tipo de delito actualmente en boga en nuestro país es el llamado **carding (**utilización de tarjetas magnéticas, ya sean hurtadas o clonadas para defraudar mediante la técnica de manipulación de datos de salida) y, el cual que es una modalidad de Fraude Informático, mismo que es considerado por la policía judicial como una clase de estafa, lo que desde el punto de vista de la clasificación típica del delito es incorrecta ya que no es una estafa, tomando en cuenta los elementos típicos de este tipo de delitos, lo que si es una clase de defraudación, pero la solución doctrinaria y típica a dicha modalidad delictual es equipararla al robo calificado, en razón que la tarjeta magnética es considerada como una llave.

4.3.5. Ley de Comercio Electrónico del Ecuador.

Desde finales de 1999 un grupo de profesionales nos vimos inmersos en la tarea de diseñar los parámetros para el surgimiento de la Ley de Comercio Electrónico del Ecuador para lo cual y tomando como guía la Ley Modelo del UNCITRAL, se creo el proyecto de ley que se puso en consideración del Congreso Nacional, el mismo que después de casi más de dos años de discusión vio la luz en Abril del 2002 dando así por fin un marco jurídico mínimo a las transacciones realizadas por medios informáticos a continuación un breve extracto del contenido de la Ley.

4.3.6. Los mensajes de datos.

Los problemas jurídicos que trae aparejado el surgimiento del comercio telemático son varios y de diversa índole. En algunos casos alcanza con la interpretación y adaptación de las normas tradicionales como las del código de comercio o el código civil, pero en otros se requiere una reforma urgente al sistema legal vigente a fin de garantizar la validez y eficacia jurídica de los Negocios en Línea.

El comercio electrónico está todavía en una etapa de formación, no sólo dentro de nuestro país, sino alrededor del mundo entero y aun no ha alcanzado a ser definido en todos sus aspectos, sin embargo sí es posible ver en forma genérica cuáles son las normas que requieren una "*Actualización Jurídica*" para estar al día con las nuevas tecnologías que posibilitan el comercio telemático.

Las páginas Web en los últimos años se han convertido en la manera más eficaz de hacer marketing y publicidad dentro de una empresa, dentro de una página Web se conjugan varios elementos decorativos y de diseño además de textos, imágenes, sonido, texturas, enlaces y cuanto elemento multimedia nos imaginemos. Cada página Web es creada en base de nuevos y novedosos diseños que la individualizan y por ende también a cada empresa para la cual se crea dicho diseño. Es en tal razón que ha surgido la necesidad de proteger esas originales creaciones intelectuales.

En este contexto cabe resaltar la iniciativa de la Oficina de Propiedad Intelectual de los Estados Unidos (Copyright Office), la cual ya registra páginas Web para efectos de brindar protección a dichas creaciones intelectuales. Los requisitos que según la Copyright Office son necesarios para el registro son los siguientes:

A. Entregar cada una de las páginas que constituyen el sitio *Web*, en forma impresa.

B. Presentar en un disquete una copia del sitio como conjunto, además de las cinco páginas más representativas de él, en forma impresa.

C. Cuando el sitio está compuesto por numerosos y complejos gráficos y enlaces (links), se deposita, además, una copia impresa en lenguaje de hipertexto de todo el sitio.

Estas nuevas iniciativas de protección de los derechos de propiedad intelectual y en especial de los derechos de autor, cada vez posibilitan que las creaciones del ingenio humano surgidas de la llamada era digital consigan el espacio y la tutela adecuada por parte no solo de los instrumentos normativos vigentes, sino de los organismos encargados de velar por su cumplimiento y aplicación. En tal sentido creo que es necesario que el IEPI (Instituto Ecuatoriano de Propiedad Intelectual) tome en cuenta estos nuevos objetos de protección a fin de que no queden aislados del amparo de las normas legales existentes.

En este sentido la ley de Defensa al Consumidor, plantea una serie de normas y reglas que bien podrían ser utilizadas en el campo del Comercio Telemático, ya que este no es más que otra forma de hacer negocios.

En tal sentido el consumidor podrá perfectamente interponer las acciones necesarias en contra de páginas WEB que tengan publicidad engañosa o abusiva de productos o servicios proporcionados por personas naturales o jurídicas legalmente establecidas en el Ecuador.

Otra garantía que brinda la nueva Ley Orgánica de Defensa al Consumidor es la facultad de devolver los bienes o servicios adquiridos por Internet siempre y cuando lo permita su naturaleza y el estado del bien sea el mismo en el que lo recibió. En el caso de servicios, el derecho se podrá ejercer mediante la cesación inmediata del contrato de provisión del servicio.

La ley trabaja sobre definiciones de equivalentes funcionales a escrito, original y firma manuscrita. Los mensajes de datos son todo lo que se transmita por una red informática. Incluye los mail, documentos, aplicaciones en sitios Web, etc. Todo se agrupa bajo esta definición. Se reconoce la validez de estas formas electrónicas en cualquier actividad, ya sea para conformar contratos perfectamente válidos o como prueba para un juicio.

En resumen lo que se busca con este título es el equivalente funcional en el medio electrónico a papel, escrito, original.

Se trabaja de modo general de forma que una vez que el documento electrónico es válido, a través de los reglamentos respectivos se le otorgarán las condiciones y requisitos a cumplir para que por ejemplo sea una factura electrónica, un voucher electrónico, una declaración de aduanas electrónica, etc.

La validez del documento se extiende incluyendo a los anexos por ejemplo cuando adjuntamos a un mail un archivo que puede contener una oferta, contrato, etc.

Para efectos legales, el documento firmado es el válido. En este caso el mensaje de datos al cual se le ha asociado una firma electrónica.

Se tipifican delitos cometidos con medios informáticos. Se establecen las sanciones con prisión y multa para diversos casos. Esto se lo hace mediante reforma al código penal ecuatoriano como corresponde.

Esta es un aparte muy importante. Se establece:

1. Que no por que exista esta ley es obligatorio aceptar la validez de lo informático. Esto siempre es prerrogativa del usuario.
2. La norma para que no se discrimine ninguna tecnología presente o futura en el tratamiento legal.
3. La declaratoria de no obligación de registro para las certificadoras.
4. La prohibición de exigir nuevos requisitos para actividades a desarrollarse en la red.
5. La obligación del Organismo Máximo de precautelar los intereses del usuario y de terceros respecto de las entidades de certificación.
6. La validez de los certificados extranjeros.

Los problemas jurídicos que trae aparejado el surgimiento del comercio telemático son varios y de diversa índole. En algunos casos alcanza con la interpretación y adaptación de las normas tradicionales como las del código de comercio o el código civil, pero en otros se requiere una reforma urgente al sistema legal vigente a fin de garantizar la validez y eficacia jurídica de los Negocios en Línea.

El comercio electrónico está todavía en una etapa de formación, no sólo dentro de nuestro país, sino alrededor del mundo entero y aún no ha alcanzado a ser definido en todos sus aspectos, sin embargo sí es posible ver en forma genérica cuáles son las normas que requieren una "Actualización Jurídica" para estar al día con las nuevas tecnologías que posibilitan el comercio telemático.

La seguridad informática en estos últimos tiempos ha alcanzado gran importancia, sobre todo en la protección de los datos personales nominativos que circulan en la red. El desarrollo de un comercio telemático fiable tendrá que contar con normas de seguridad que permitan proteger la información almacenada en computadores conectados a la red. En este sentido el valor que tiene dicha información en estos momentos se puede equiparar al valor que tiene cualquier bien corporal o material. En tal razón es necesario que nuestra legislación prevea sanciones en caso de que la información que transite por la red sea interceptada o captada con el fin de perjudicarnos, es así como se manifestó en líneas anteriores en Ley de Comercio Electrónico se realiza una reforma al Código Penal para de tipificar los llamados delitos informáticos a fin de que el comercio electrónico no solo posea una seguridad técnica como puede ser el uso de servidores seguros o sistemas de encriptación sino que también tengamos una seguridad normativa que nos permita actuar en caso de la agresión de este nuevo bien jurídico llamado información.

Garantizar la protección de la información que se transmite a través del comercio electrónico a fin de resguardar el derecho a la intimidad y de la

confidencialidad o reserva será un gran desafío de acuerdo a los importantes intereses comprometidos

Las modernas herramientas informáticas permiten al hombre acumular una gran cantidad de información, pero no solo eso, las computadoras hoy en día pueden realizar búsquedas sistemáticas, analizar, ordenar, sintetizar la información contenida en sus bases de datos, lo que da la medida que en muy pocos segundos la computadora puede dar un perfil completo de una persona cualquiera, solamente relacionando lo que se ha dado en llamar "**datos nominativos**[36]**"**, los cuales son la información personal tratada por medios informáticos.

Sin embargo, y sin desconocer aquellos beneficios que la tecnología puede proporcionar, el tratamiento computarizado de información puede llegar a constituir en algunos casos una verdadera invasión al derecho a la intimidad y demás libertades individuales relacionadas con ellas.

En tal razón en nuestro país se deben implementar una serie de normas tendientes a proteger los datos personales que se encuentran distribuidos tanto en bases públicas como privadas a fin de que se genere un marco mínimo de regulación que permita por un lado la protección de datos personales y por el otro que no sea un obstáculo para el desarrollo del comercio telemático.

También el derecho de los consumidores requiere un examen profundo para

[36] **JIJENA LEIVA, Renato,** Chile: Protección Penal a la Intimidad y los Delitos Informáticos, Editorial Jurídica de Chile, 1993.

indagar si las leyes actuales podrán prevenir fraudes o incumplimiento de contratos celebrados por computador. Proteger a los consumidores de eventuales prácticas defraudatorias va a requerir una reformulación de las políticas instrumentadas para su amparo en el mundo material. Esto resulta importante porque sin seguridad el comercio electrónico no va a ser atractivo para los consumidores.

En este sentido la ley de Defensa al Consumidor, plantea una serie de normas y reglas que bien podrían ser utilizadas en el campo del Comercio Telemático, ya que este no es más que otra forma de hacer negocios.

En tal sentido el consumidor podrá perfectamente interponer las acciones necesarias en contra de páginas Web que tengan publicidad engañosa o abusiva de productos o servicios proporcionados por personas naturales o jurídicas legalmente establecidas en el Ecuador.

Otra garantía que brinda la nueva Ley Orgánica de Defensa al Consumidor es la facultad de devolver los bienes o servicios adquiridos por Internet siempre y cuando lo permita su naturaleza y el estado del bien sea el mismo en el que lo recibió. En el caso de servicios, el derecho se podrá ejercer mediante la cesación inmediata del contrato de provisión del servicio.

Este tipo de infracciones son difícilmente descubiertas o perseguidas ya que los sujetos activos actúan sigilosamente, y poseen herramientas capaces de borrar todo rastro de intrusión o la consumación del delito, pero a pesar de eso y de no contar ni con una policía entrenada para investigar dichos hechos, ni un Ministerio Público que pueda dar las directrices para la

correcta indagación de dichos actos delictivos, por no contar entre otras con una Unidad Especial para la investigación y persecución de estas infracciones informáticas, existen dos problemas principales que a continuación se exponen:

Esta característica de transnacional de la delincuencia informática es otro de los problemas de perseguibilidad. Tradicionalmente se ha considerado que la ley penal solo se aplica en el territorio de la República, hecho que constituye el llamado "principio de territorialidad de la ley", el mismo que se encuentra tipificado como ya se mencionó en el art. 5 del Código Penal. El principio de territorialidad sostiene que la ley penal de un país es aplicable cuando la infracción ha sido cometida dentro del territorio, en el momento actual esto puede haber cambiado teniendo en cuenta que el nuevo escenario en donde mayormente se da este tipo de delitos es el Ciberespacio, un lugar donde no existen fronteras territoriales, y que de acuerdo a **Jhon Perry Barlow**, quien público lo que se llama **LA DECLARACIÓN DE INDEPENDENCIA DEL CIBERESPACIO**, en donde manifiesta: *"Gobiernos del mundo industrializado, gigantes obsoletos , de la nueva morada del espíritu (...) No os queremos entre nosotros, en el terreno donde nos reunimos no sois soberanos.. Vuestros conceptos jurídicos de propiedad, de expresión, de identidad, de movimiento y de contexto no se aplican a nosotros. Están basados en la materia"*[37]

Por lo dicho se puede constatar de prima facie que es difícil la persecución

[37] **BARLOW, Jhon Perry,** Publicación hecha en el sitio Web: www.eff.org/pub/publications/Jhon_perry_barlow/barlow_0296

de estos delitos y su enjuiciamiento, ya que existe la posibilidad de preparar y cometer acciones delictivas informáticas en perjuicio de terceros en tiempo y espacio lejanos.

Debido a los adelantos de las telecomunicaciones y la telemática, hace que las distancias reales o fronteras entre países no existan como ya se ha dicho, ya que una persona puede realizar un acto delictivo en un lugar distinto del lugar de los hechos, como por ejemplo los creadores de MALWARE o de los VIRUS INFORMÁTICOS como el conocido: I LOVE YOU, el mismo que fue diseñado y creado en Filipinas y causó daños a nivel mundial en cuestión de días. Por otro lado, la posibilidad de realizar programas de efecto retardado como las llamadas bombas lógicas, las cuales no desatan su poder destructivo, hasta tiempo después de que el autor material de la infracción este a "buen recaudo"; o que con determinadas ordenes, rutinas y subrutinas de algunos programas se puede preparar el cometimiento de una infracción como la del fraude informático, y en el momento que esto sucede el hechor se encuentra realizando una tarea completamente incompatible con el acto delictivo cometido.

La territorialidad de la ley es considerada como un principio de soberanía del estado y se resume al decir que no se puede aplicar al ecuatoriano delincuente otra ley que no sea la ecuatoriana, aclarando que no importa el lugar donde se encuentre el delincuente, es decir, sin importar el país en donde se haya cometido el delito.

Este principio denota algunas características como las siguientes:

❖ La ley penal es aplicable a los hechos punibles cometidos dentro del territorio del Estado, sin consideración a la nacionalidad del actor.

❖ No se toma en cuenta la nacionalidad del autor.

❖ Se toma en cuenta el lugar de comisión del delito. Nuestra legislación se inclina por la teoría del resultado, es decir que la INFRACCIÓN se entiende cometida en el territorio del Estado cuando los *efectos de la acción u omisión* deban producirse en el Ecuador o en los lugares sometidos a su jurisdicción.

❖ Se aplica al concepto jurídico de territorio por el Derecho Internacional: los límites del Estado, mar territorial. Espacio aéreo.

❖ Se aplica también la teoría del **territorio flotante** o **Principio de la bandera**: Naves o aeronaves de bandera nacional ya sea que se encuentren en alta mar, en su espacio aéreo y en lugares en que por la existencia de un convenio internacional, ejerzan jurisdicción. Este principio no se aplica cuando las naves o aeronaves MERCANTES ESTÉN SUJETAS A UNA LEY PENAL EXTRANJERA.

El ámbito de aplicación de este principio está en:

1.- Territorio Continental

2.- Espacio Aéreo

3.- Mar Territorial

4.- Naves y aeronaves ecuatorianas de guerra o mercantes.

5.- Infracciones cometidas en el recinto de una **Legación ecuatoriana en país extranjero.**

Tres son los principios que constituyen el principio de extraterritorialidad y son los siguientes: el principio de la nacionalidad o personalidad, el principio de la defensa y el principio de la universalidad y justicia mundial.

A.- Principio de la nacionalidad o personalidad.

Según este, se debe aplicar al delincuente únicamente la ley que corresponde a su nacionalidad, es decir, la ley del país de su origen, sea el país que sea en el que haya cometido el delito. Este principio tiene dos divisiones:

PRINCIPIO DE LA NACIONALIDAD ACTIVA.- Se funda en la obediencia que se exige al súbdito ecuatoriano con respecto a su legislación. Se toma en cuenta la nacionalidad del autor del delito.

PRINCIPIO DE LA NACIONALIDAD PASIVA.- El alcance espacial de la ley se extiende en función *del ofendido o titular del bien jurídico protegido.* Se aplicaría cuando está en juego la protección de los bienes jurídicos individuales

B.- Principio de la defensa.-

Este nos dice que es aplicable la ley del país donde los principios son atacados por el delito, sin tomar en cuenta la nacionalidad de los realizadores. Se toma en cuenta la nacionalidad del bien jurídico protegido, es decir se aplica este principio cuando se afecta la integridad territorial. Quedando en juego la protección de los bienes nacionales. Ha sido tomado por algunos países, como por ejemplo el nuestro el cual puede pedir la extradición de una delincuente informático que haya vulnerado bienes

jurídicos protegidos en nuestro país como resultado de su acción delictiva. Claro que esta norma no puede ser aplicada en todos los países ya que algunos de ellos como el nuestro prohíbe la extradición de ecuatorianos que hayan cometido una infracción en otro país, en este caso se aplica un principio de equivalencia, es decir si el delito cometido en el otro país se encuentra tipificado en el nuestro también puede seguirse el proceso penal por el cometimiento de dicho delito, pero en nuestro país.

C.- Principio de la universalidad y justicia mundial.

Este principio se refiere a que es aplicable la ley del país que primero aprese al delincuente, sin considerar otro aspecto.

Este principio tiene una finalidad práctica para reprimir los delitos contra la humanidad, aquellos que han sido catalogados como tales en virtud de ser considerados como ofensores de toda la humanidad. Para ello es necesario firmar convenios internacionales y unilaterales con el fin de que cada país pueda sancionar al delincuente con su propia ley, sin importar el lugar donde el individuo haya cometido el acto ni tampoco la nacionalidad del mismo.

Se prescinde tanto de la nacionalidad del autor como del lugar de comisión del delito, se fundamenta en el principio de **solidaridad de los estados en la lucha contra el delito.**

En doctrina penal se concede en virtud de este principio eficacia extraterritorial a la ley penal; pero en el Derecho Internacional condiciona esta eficacia extraterritorial tomando en cuenta:

- La calidad del bien jurídico protegido, como bienes culturales supranacionales.
- Cuando los autores del delito sean peligrosos para todos los estados.

En cuanto a los delitos informáticos de carácter transnacional, en especial el Ciberterrorismo es necesario aplicar este principio por cuanto la peligrosidad de este tipo de ataques puede causar más daño que el terrorismo convencional.

El sujeto activo de esta clase de infracciones puede ser totalmente anónimo y usar este anonimato como forma de evadir su responsabilidad, ya que este no necesariamente puede usar su propio sistema informático, sino que se puede valer de un tercero, como por ejemplo en el caso del envión de correo no deseado o SPAM, en el cual se puede usar a una máquina zombi, es decir una computadora que está bajo el control del SPAMER y que le permite usarla como una estación de trabajo de su propia red de máquinas zombis, las cuales pertenecen a usuarios desaprensivos que no tienen al día sus medidas de seguridad y que son fácil presa de los hackers y crakers para cometer este tipo de infracciones. También existen programas de enmascaramiento o que no permiten ver la verdadera dirección ya sea de correo electrónico o del numero IP.

4.4. LEGISLACION COMPARADA.

Durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

En un primer término, debe considerarse que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de pena.

4.4.1. Alemania.

En Alemania, para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la

Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

- Espionaje de datos (202 a)
- Estafa informática (263 a)
- Falsificación de datos probatorios(269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(270, 271, 273)
- Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.
- Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, Inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b)

Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, producción del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de

una intervención ilícita.

Sobre el particular, cabe mencionar que esta solución en forma parcialmente abreviada fue también adoptada en los Países Escandinavos y en Austria.

En opinión de estudiosos de la materia, el legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como los Estados Unidos. De esta forma, dicen que no solo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de procesos de datos, aunque tenga lugar de forma cualificada.

En el caso de Alemania, se ha señalado que a la hora de introducir nuevos preceptos penales para la represión de la llamada criminalidad informática el gobierno tuvo que reflexionar acerca de dónde radicaban las verdaderas dificultades para la aplicación del Derecho penal tradicional a comportamientos dañosos en los que desempeña un papel esencial la introducción del proceso electrónico de datos, así como acerca de qué bienes jurídicos merecedores de protección penal resultaban así lesionados.

Fue entonces cuando se comprobó que, por una parte, en la medida en que las instalaciones de tratamiento electrónico de datos son utilizadas para la comisión de hechos delictivos, en especial en el ámbito económico, pueden conferir a éstos una nueva dimensión, pero que en realidad tan solo constituyen un nuevo modus operandi, que no ofrece problemas para la aplicación de determinados tipos.

Por otra parte, sin embargo, la protección fragmentaria de determinados bienes jurídicos ha puesto de relieve que éstos no pueden ser protegidos suficientemente por el Derecho vigente contra nuevas formas de agresión que pasan por la utilización abusiva de instalaciones informáticas.

En otro orden de ideas, las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra menoscabos de su sustancia o función de alteraciones de su forma de aparición.

4.4.2. Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987. Esta ley contempla los siguientes delitos:

- Destrucción de datos (126). En este artículo se regulan no solo los datos personales sino también los no personales y los programas.
- Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

4.4.3. Estados Unidos

Consideramos importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya, etcétera y en qué difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas. (18 U.S.C.: Sec. 1030 (a) (5) (A). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus, de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten solo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

Nos llama la atención que el Acta de 1994 aclara que el creador de un virus no puede escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus

informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Consideramos importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10, 000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos, etcétera.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era el de aumentar la protección a los individuos, negocios y agencias gubernamentales de la interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el

bienestar de las instituciones financieras, de negocios, agencias gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

4.4.4. Chile.

En junio de 1993 entró en vigencia en Chile la Ley n°19.223, sobre delitos informáticos.- La Ley Nº 19.223 tiene como finalidad proteger a un nuevo bien jurídico como es: "la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan".

La Ley n°19.223, es una ley especial, extra código y consta de 4 artículos, que se enuncian a continuación.

Artículo 1. "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

Artículo 2. "El que con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".

Artículo 3. “El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio”.

Artículo 4. “El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado”.

En la Ley no. 19.223 se contemplaría los delitos informáticos de sabotaje y espionaje informáticos, aunque no de una forma clara. Así pues, en el artículo 1, el inciso primero alude a los daños que se puedan cometer contra el hardware, sea destruyéndolo o inutilizándolo, por lo que no se trataría de un delito informático sino más bien de un delito de daños convencional. Es en el artículo 3° es en donde encontraríamos la figura del sabotaje informático al sancionar al que maliciosamente altere, dañe o destruya los datos contenidos en un sistema.

Por su parte, el espionaje informático se tipificaría en el artículo 2 y 4. En este último caso, el tipo es demasiado amplio y no otorga un valor determinado a los datos afectados, dando, a mi parecer, un tratamiento inadecuado.

En la Ley no. 19.223, no se contemplan figuras como el hacking o el fraude informático.

En cuanto a la penalidad, esta ley establece según el artículo 1, por ejemplo,

en el caso de que alguien destruya dolosamente un computador, puede recibir como castigo la pena de presidio menor en su grado medio a máximo, es decir, puede tener desde 541 días hasta 5 años de cárcel. En virtud del artículo 2, si un hacker, por ejemplo, ingresa indebidamente a un sistema para conocer información sin autorización, puede recibir desde 61 días hasta 3 años de presidio. De acuerdo al artículo 3, si alguien, por ejemplo, graba intencionalmente un virus en un sistema, puede ser castigado desde 541 días hasta 3 años de presidio. Finalmente, en virtud del artículo 4, podría recibir también presidio desde 541 días hasta 3 años, un operador que dé a conocer dolosamente el contenido de la información guardada en el sistema informático, e incluso podría alcanzar hasta 5 años si la persona es el responsable del sistema.

En conclusión podemos decir que son evidentes las falencias en las que incurre la ley chilena respecto a la regulación de la Delincuencia Informática, no obstante hay que señalar que la Ley n°19.223, es la pionera en la región al abordar expresamente el tema de los delitos informáticos.

5. MATERIALES Y MÉTODOS

Para la realización del presente trabajo de investigación jurídica, referente a la **"NECESIDAD DE REFORMAR LA LEY DE COMERCIO ELECTRÓNICO CON LA FINALIDAD DE ESTABLECER UNA PENA CONTRA LOS MENSAJES DE DATOS DE COMUNICACIÓN NO SOLICITADA DE PRODUCTOS Y SERVICIOS"**, se utilizamos el método científico y dentro de él y como métodos auxiliares se utilizamos la inducción que intenta obtener de los casos particulares observados una ley general válida también para los no observados. De esta manera se analizó el problema como parte principal del estudio lo que nos ayudó a realizar un análisis crítico de los aspectos que lo constituyen y lo rodean.

Aplicamos además algunas referencias históricas para lo cual se hizo uso del materialismo histórico lo que permitió conocer los aspectos que encierran la evolución histórica desde los inicios del universo hasta los actuales momentos, para caracterizar objetivamente el tema planteado con la finalidad de entenderlo como un proceso histórico que aún sigue evolucionando en todos sus aspectos.

En lo referente a las técnicas de investigación, utilizamos, las siguientes técnicas:

Lectura científica.- Para recolectar datos de la bibliografía especializada de una manera objetiva.

Encuestas.- Con esta técnica investigativa obtendré la información mediante un cuestionario de preguntas aplicadas a un determinado grupo social o

universo, en este caso, la encuesta se dirigió a los señores Abogados en libre ejercicio profesional. La información recogida la tabulamos manualmente para obtener datos estadísticos para verificar la hipótesis planteada.

Con la finalidad de obtener suficiente información que nos permita desarrollar el sumario de la investigación jurídica, utilizamos la técnica del fichaje, con fichas bibliográficas, hemerográficas y mnemotécnicas.

Recogida toda la información, la analizamos objetivamente mediante tablas y cuadros estadísticos, para verificar los objetivos e hipótesis y para el planteamiento de las conclusiones y recomendaciones y de la propuesta jurídica de reforma.

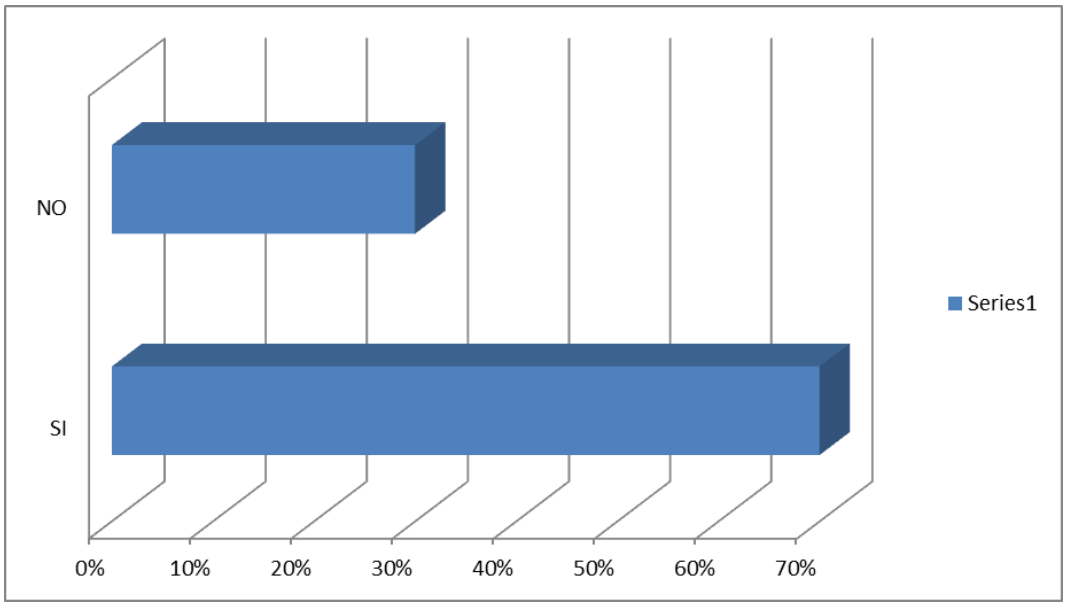
6. RESULTADOS

Cumpliendo con lo establecido en el cronograma de trabajo se aplicaron treinta encuestas a Abogados en libre ejercicio profesional, los resultados obtenidos son los siguientes:

PRIMERA PREGUNTA:

¿Considera usted que es necesario que en nuestro país, se mantenga una actualización constante de la normativa legal en lo referente a la protección de los derechos de las personas en general?

VARIABLE	FRECUENCIA	PORCENTAJE
SI	21	70%
NO	9	30%
TOTAL	**30**	**100%**

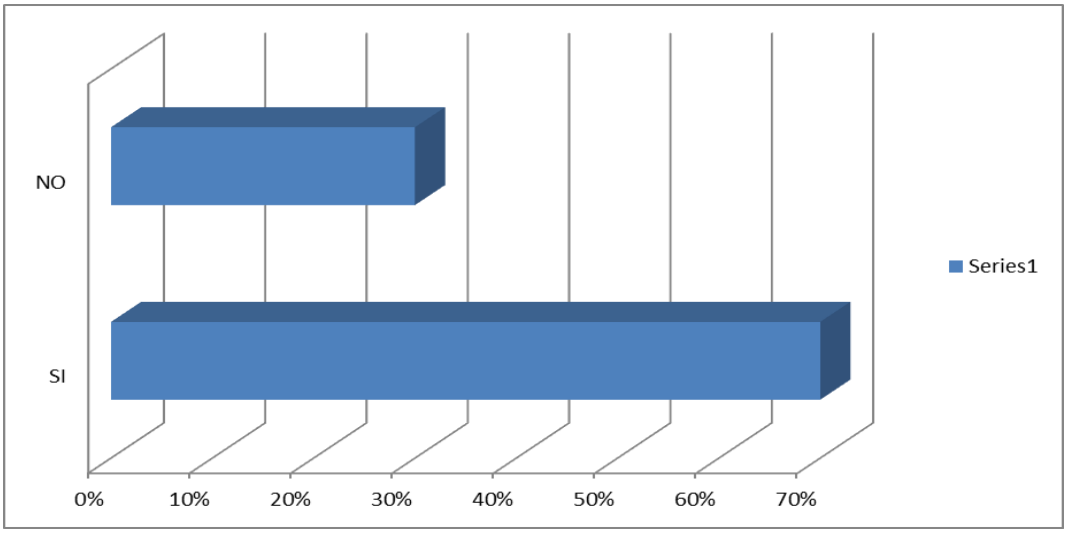


Análisis de los Datos: A esta pregunta el 70% de los encuestados contestan afirmativamente; señalando que los derechos de las personas, deben ser constantemente protegidos a través de disposiciones normativas viables; por su parte el 30% restante contesta negativamente, señalando que no es necesaria una revisión constante de las normas sino una aplicación definitiva en todos los estamentos del estado

SEGUNDA PREGUNTA:

¿En el mismo sentido de la pregunta anterior, según su criterio cree usted que los derechos de las personas a la intimidad se ven constantemente afectados por acciones realizadas a través del uso del internet?

VARIABLE	FRECUENCIA	PORCENTAJE
SI	21	70%
NO	9	30%
TOTAL	**30**	**100%**

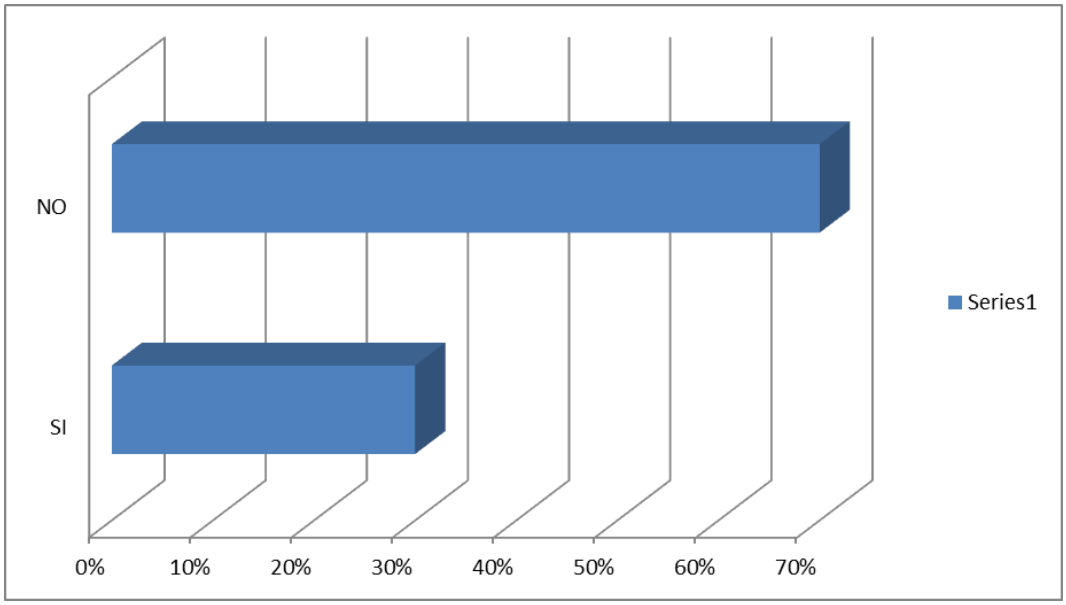


Análisis de los Datos: En esta pregunta el 70% de encuestados afirma que en efecto el derecho a la intimidad se ve constantemente acechados con la recepción de mensajes no deseados más conocidos como spam; mientras que un 30% señala que los derechos previstos a la intimidad se ven acechados más por acciones políticas que por acciones de personas ajenas.

TERCERA PREGUNTA

¿Según su criterio, el Estado ha cumplido eficazmente con su responsabilidad de frenar la comunicación no solicitada de productos y servicios en el país; a través del internet?

VARIABLE	FRECUENCIA	PORCENTAJE
NO	21	70%
SI	9	30%
TOTAL	**30**	**100%**

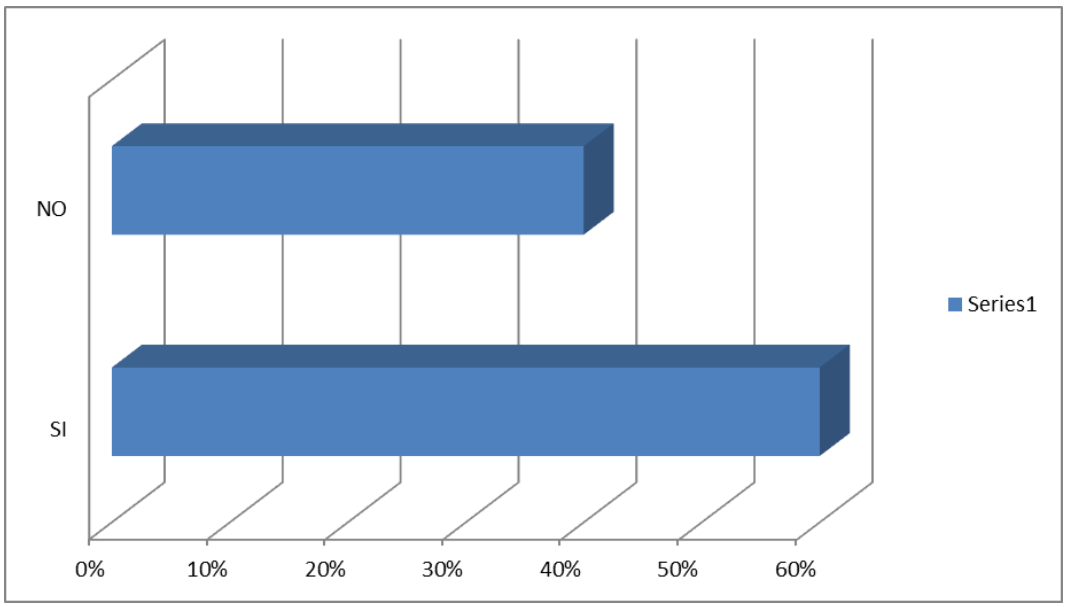


Análisis de los Datos: El 70% de los encuestados, señala que el Estado hasta la fecha no ha tenido acciones concluyentes que permitan una protección eficaz de los derechos de las personas, a través de la comisión de los delitos informáticos; mientras que el 30% restante señala que si ha cumplido no en un porcentaje totalmente eficiente pero la adopción de convenios, tratados y normas nuevas permitan una mejor protección.

CUARTA PREGUNTA

¿Considera usted que siendo el spam un mensaje de datos no solicitado que atenta al derecho a la intimidad, debe regularse como una conducta delictiva?

VARIABLE	PORCENTAJE	FRECUENCIA
SI	60%	18
NO	40%	16
TOTAL	**100%**	**30**

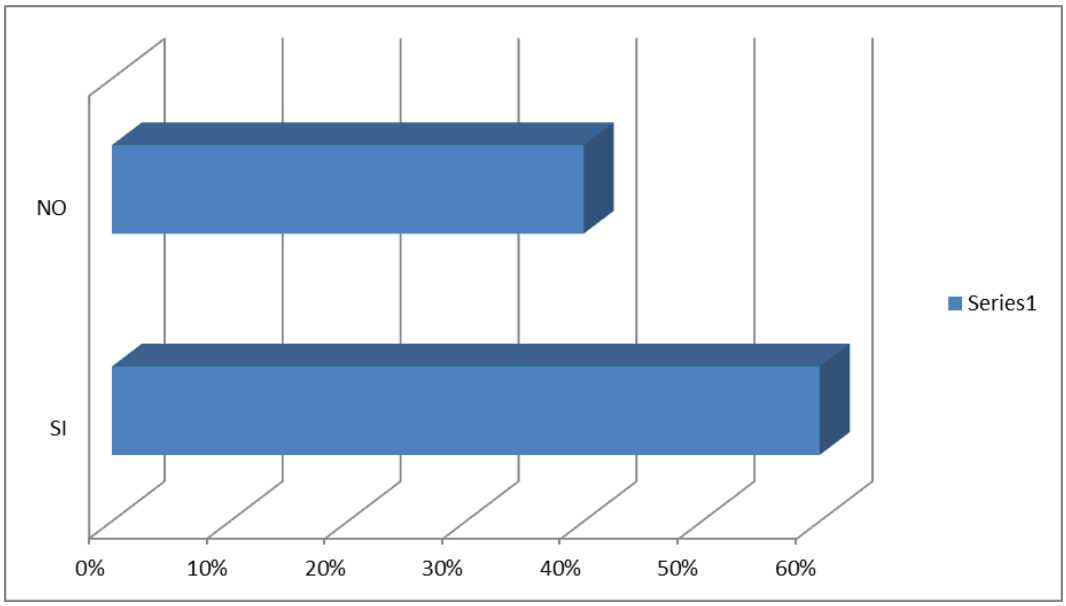


Análisis de los Datos: A esta pregunta el 60% determina que algunas conductas informáticas deben considerarse como delitos informáticos incluido el envío de spam; mientras que el 40% restante considera que en el nuevo Código Orgánico Integral Penal ya se regula suficientemente al respecto.

QUINTA PREGUNTA:

¿Según su criterio considera usted que el envío de mensajes de datos no solicitados o spam, debe sancionarse también en la Ley de Comercio Electrónico a efectos de frenar esta acción delictiva?

VARIABLE	PORCENTAJE	FRECUENCIA
SI	60%	18
NO	40%	16
TOTAL	**100%**	**30**

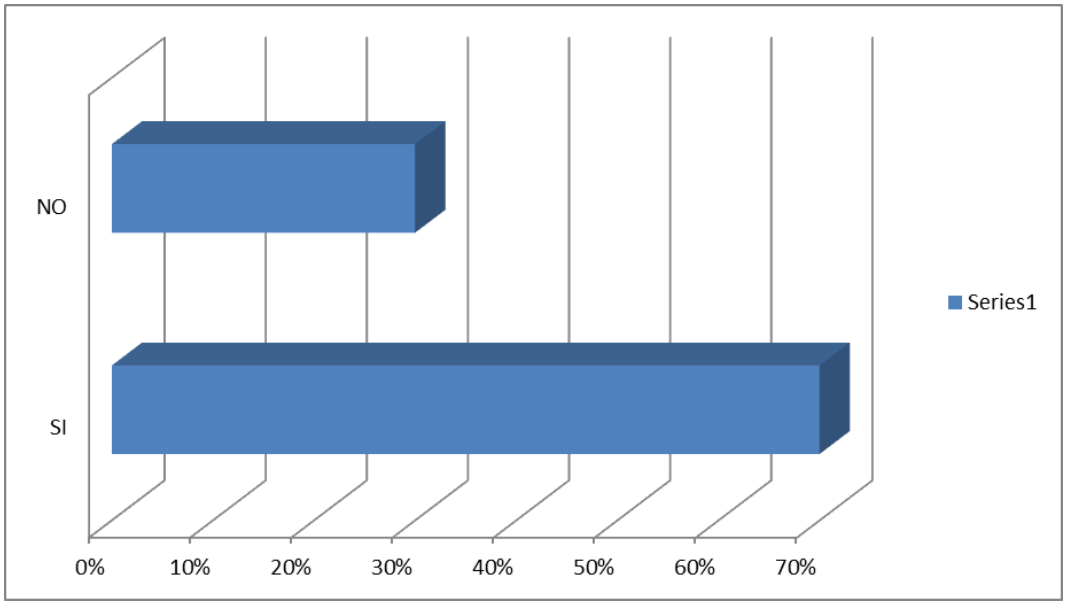


Análisis de los Datos: En esta pregunta el 60% del total de encuestados, señala que si debe regularse en la ley de Comercio Electrónico el envío de spam como una conducta ilícita; mientras que el 40% restante señala que si debe regularse pero no en la Ley de Comercio Electrónico.

SEXTA PREGUNTA:

¿Considera usted que es necesario que en la ley de Comercio Electrónico y Mensajes de Datos, así como en su reglamento, se regule de debida forma, una sanción administrativa y penal al envío de mensajes de datos no autorizados?

VARIABLE	FRECUENCIA	PORCENTAJE
SI	21	70%
NO	9	30%
TOTAL	**30**	**100%**

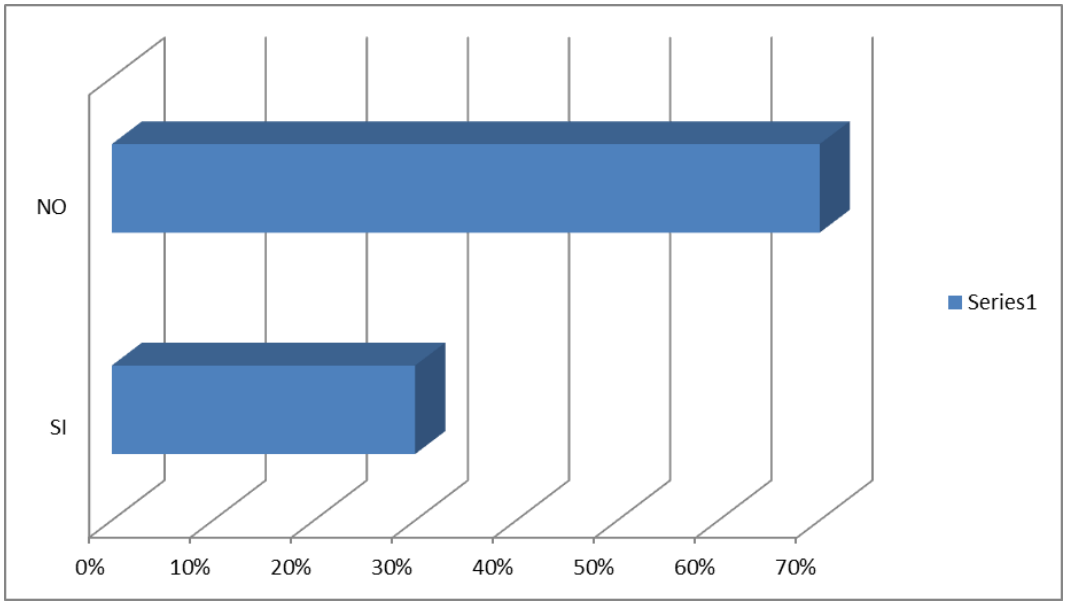


Análisis de los Datos: A esta pregunta el 70% de los encuestados contestan afirmativamente; señalando que si se debe sancionar a efectos de reducir el abuso del internet para promocionar productos y servicios no queridos; por su parte el 30% restante contesta negativamente, señalando que no es posible ya que eso significaría dejar sin efecto el Art. 22 de la Ley de Mensaje de datos.

SEPTIMA PREGUNTA

¿En su experiencia considera usted que la norma del Art. 22 del Reglamento a la Ley de Mensaje de Datos impide sanciones eficaces al envio de mensajes de datos?

VARIABLE	FRECUENCIA	PORCENTAJE
NO	21	70%
SI	9	30%
TOTAL	**30**	**100%**

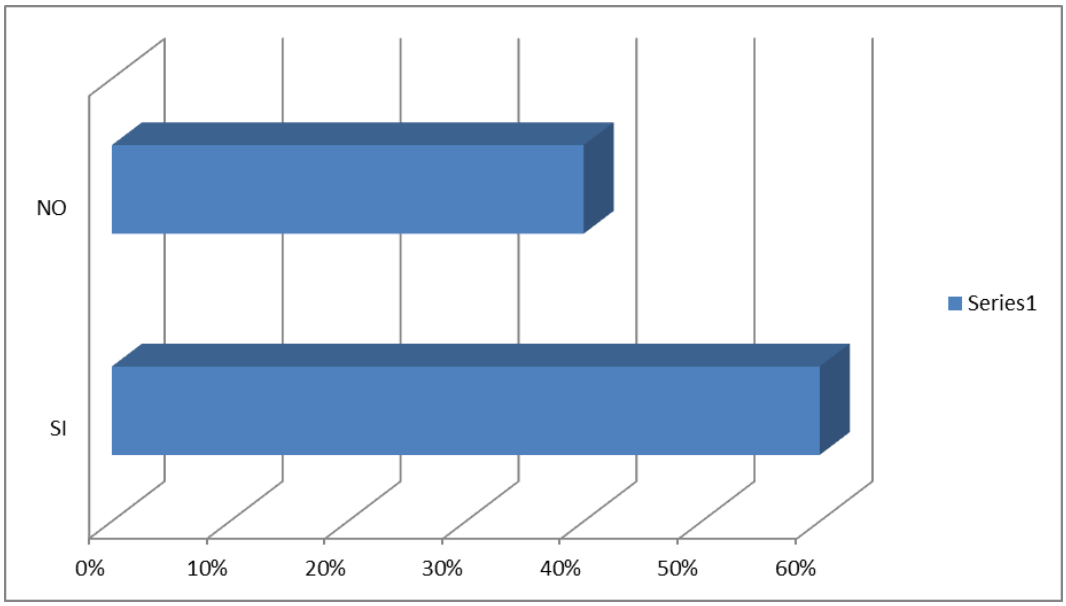


Análisis de los Datos: El 70% de los encuestados, señala que no necesariamente ya que de incumplirse con las condiciones previstas en esa norma entonces se la violentaría y requerirá una sanción; mientras que el 30% restante señala que si definitivamente constituye un impedimento que requiere subsanarse.

OCTAVA PREGUNTA

¿Considera usted que es necesario entonces una reforma a varios cuerpos legales, es decir a la Ley de Comercio electrónico pero tambien a su reglamento?

VARIABLE	PORCENTAJE	FRECUENCIA
SI	60%	18
NO	40%	16
TOTAL	**100%**	**30**



Análisis de los Datos: A esta pregunta el 60% determina que en efecto una reforma debe ser regular y constante a varios cuerpos legales como los mencionados; mientras que el 40% restante considera que no es necesario la ley es la base fundamental de aplicación y ahí deben constar las sanciones.

7. DISCUSIÓN

7.1. Verificación de objetivos y contrastación de hipótesis

El Objetivo general planteado, así como los objetivos específicos han sido comprobados en su totalidad, para conseguirlo fue necesario examinar detenidamente la legislación de comercio electrónico, así como la Constitución del Estado.

Este estudio pormenorizado de los acotados cuerpos normativos nos permitió tener en claro que el envío de mensajes de datos no solicitados considerado como spam, deben contenerse como una acción ilícita.

Como consecuencia del análisis crítico realizado para alcanzar el objetivo general propuesto, llegamos a detectar la necesidad de analizar la ley con claridad sobre todo en lo referente a la necesidad de reformar la Ley de Comercio Electrónico en lo referente al envío de mensajes de datos no solicitados.

De acuerdo a las Hipótesis propuesta:

- La falta de una sanción en la Ley de Comercio Electrónico para toda persona que incluyere de forma no solicitada información y publicidad en los correos electrónicos y teléfonos celulares, atenta contra el derecho de las personas a la intimidad personal, y causa confusión entre las personas ya que en muchas de las veces se tratan de fraude y engaño.

En el presente trabajo puedo decir que también la he verificado

positivamente, de hecho, la falta de sanciones en la Ley de Comercio Electrónico más bien viabiliza el envío de mensajes de datos, lo cual debe reformarse.

7.2. Fundamentos que sustentan la propuesta

Como resultado del proceso de globalización y la difusión de la tecnología, se están produciendo cambios significativos en la naturaleza y el alcance de la delincuencia organizada. Una tendencia clave es la diversificación de las actividades ilícitas que realizan los grupos delictivos organizados, así como un aumento del número de países afectados por la delincuencia organizada. También se ha producido una expansión rápida de tales actividades en esferas como la trata de personas, el tráfico ilícito de armas de fuego, vehículos robados, recursos naturales, objetos culturales, sustancias que agotan la capa de ozono, desechos peligrosos, especies amenazadas de fauna y flora silvestres e incluso órganos humanos, así como el secuestro para la obtención de un rescate.

Los adelantos en la tecnología de las comunicaciones han determinado que surgieran nuevas oportunidades para la comisión de delitos sumamente complejos, en particular un aumento significativo del fraude en la Internet, y esas oportunidades han sido explotadas por los grupos delictivos organizados. La tecnología de las comunicaciones también confiere más flexibilidad y dinamismo a las organizaciones delictivas; el correo electrónico se ha convertido en un instrumento de comunicación esencial independiente del tiempo y la distancia.

Las autoridades encargadas de hacer cumplir la ley suelen adaptarse con lentitud a las nuevas tendencias, mientras que los grupos delictivos organizados tienden a adaptarse rápidamente y a aprovechar los adelantos tecnológicos debido a los inmensos beneficios que producen sus actividades ilícitas.

La apertura de nuevos mercados y las nuevas tecnologías de las comunicaciones, junto con la diversidad de actividades en las que participan, también han alimentado el crecimiento de la delincuencia organizada en los países en desarrollo. Los países con economías en transición o en situaciones de conflicto son particularmente vulnerables al crecimiento de ese tipo de delincuencia. En tales casos, la delincuencia organizada plantea una amenaza real para el desarrollo de instituciones reformadas, como la policía, los servicios de aduana y el poder judicial, que pueden adoptar prácticas delictivas y corruptas, planteando un grave obstáculo al logro de sociedades estables y más prósperas.

La delincuencia organizada y las prácticas corruptas van de la mano: la corrupción facilita las actividades ilícitas y dificulta las intervenciones de los organismos encargados de hacer cumplir la ley. La lucha contra la corrupción es, por lo tanto, esencial para combatir la delincuencia organizada. Es más, se ha establecido un nexo entre la delincuencia organizada, la corrupción y el terrorismo. Algunos grupos terroristas, por ejemplo, han recurrido a la delincuencia organizada para financiar sus actividades. Por consiguiente, la promulgación de legislación apropiada, el fomento de la capacidad de hacer cumplir la ley y la promoción de la

cooperación internacional para luchar contra las actividades de la delincuencia organizada y las prácticas corruptas conexas también fortalecen la capacidad de combatir el terrorismo.

8. CONCLUSIONES

Al finalizar la presente investigación, hemos llegado a las siguientes conclusiones:

- Comercio Electrónico o Telemático es: Es toda transacción telemática de información realizada mediante el uso de mensajes de datos, de carácter gratuito u oneroso entre dos o más personas que da como resultado una relación comercial, civil, financiera, bursátil o de cualquier otra índole consistente en la adquisición de bienes tangibles, intangibles, o la prestación de un servicio.
- Los mensajes de datos son un concepto propio de las firmas digitales en los que se entiende como tal a cualquier tipo de mensaje enviado o recibido por medio electrónico u óptico. Por lo general se entiende a comunicaciones efectuadas mediante correo electrónico; sin embargo, también se extiende a otras comunicaciones como el telegrama, el telex o el telefax.
- El ser humano poco a poco, logró automatizar muchas de sus actividades. Se ahorra tiempo y recursos con el empleo de lo que se denomina "inteligencia artificial". Es difícil imaginar alguna actividad humana en la que no intervengan máquinas dotadas de gran poder de resolución.
- En nuestro país, el fenómeno de la criminalidad informática o de los llamados delitos informáticos, no han alcanzado todavía una importancia mayor, esto por cuanto no se conoce en nuestro entorno mucho sobre esta clase de infracciones a pesar del efecto de aldea global que estamos viviendo, y la razón de que esta nueva forma de lesión a bienes jurídicos

tutelados no sea tomada en cuenta, es porque se ha perdido por parte de la legislación penal nacional la conexión entre ésta y la realidad social actual.

- En derecho penal, la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito. Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero.
- El problema que se advierte por parte de las instituciones llamadas a perseguir las llamadas infracciones informáticas es la falta de preparación en el orden técnico tanto del Ministerio Público como de la Policía Judicial, esto en razón de la falta por un lado de la infraestructura necesaria, como centros de vigilancia computarizada, las modernas herramientas de software y todos los demás implementos tecnológicos necesarios para la persecución de los llamados Delitos Informáticos
- Los problemas jurídicos que trae aparejado el surgimiento del comercio telemático son varios y de diversa índole. En algunos casos alcanza con la interpretación y adaptación de las normas tradicionales como las del código de comercio o el código civil, pero en otros se requiere una reforma urgente al sistema legal vigente a fin de garantizar la validez y eficacia jurídica de los Negocios en Línea.
- El comercio electrónico está todavía en una etapa de formación, no sólo dentro de nuestro país, sino alrededor del mundo entero y aún no ha alcanzado a ser definido en todos sus aspectos, sin embargo sí es posible ver

en forma genérica cuáles son las normas que requieren una “Actualización Jurídica” para estar al día con las nuevas tecnologías que posibilitan el comercio telemático.

9. RECOMENDACIONES

Podemos resumir nuestra propuesta de la siguiente manera:

- Es necesario establecer con claridad cada uno de los componentes de los delitos informáticos a efectos de poder regular de mejor manera lo referente a la determinación de todos sus aspectos no solamente en la Ley penal sino además en la ley de Comercio Electrónico.
- El Estado debe propiciar la determinación de políticas públicas urgentes destinadas a frenar la comisión de delitos informáticos por medios electrónicos; el envío de mensajes de datos sin autorización para promocionar productos o servicios, es otro aspecto que debe determinarse dentro de los delitos informáticos, y que requiere atención urgente.
- Para establecer una eficaz reforma respecto del problema investigado, la misma debe realizarse a todo cuerpo legal relacionado, por ello es necesario que la Asamblea Nacional reforme tanto el Código Orgánico Integral Penal como la Ley de Comercio Electrónico y su reglamento.
- Es necesario además que a todo nivel se emprenda en acciones coincidentes y concordantes a efectos de lograr el establecimientos de controles permanentes en el cometimiento de delitos informáticos, nuestro país, no cuenta con elementos necesarios para hacer frente a este tipo de delitos, por lo que se requiere entonces, el apoyo de todos los estamentos institucionales del estado y propender acciones conjuntas que permitan la detección temprana de estos delitos así como su juzgamiento.

9.1. PROPUESTA DE REFORMA

PROPUESTA DE REFORMA A LA LEY DE COMERCIO ELECTRÓNICO

La Honorable Asamblea Nacional,

Considerando:

Que es deber del Estado procurar el cumplimiento de sus normas constitucionales y por tanto garantizar la inviolabilidad de dichas garantías principalmente en lo que respecta a las libertades constitucionales;

En uso de las facultades previstas en el Art. 120 numeral 6 de la Constitución Política del Ecuador, expide el siguiente:

Expide:

La siguiente Ley reformatoria a la Ley de Comercio Electrónica

Art.- 1.- Sustitúyase el Art. 57 de la Ley de Comercio Electrónico:

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Orgánico Integral Penal; y, a la presente ley. Estas infracciones informáticas se sancionarán con el máximo de las penas previstas en el Código Integral penal, especialmente para el envío de mensajes de datos.

Art.- 2.- Después del Art. 57 de la Ley de Comercio Electrónico, agréguese el siguiente artículo innumerado:

Art.-….- Serán reprimidos con prisión de un año y multa de diez salarios mínimos vitales los representantes de las Instituciones públicas como privadas que expongan informaciones falsas sobre la integridad física, psíquica, moral o sexual de una persona sin su consentimiento".

Es dado y firmado en la Sala de Sesiones del Honorable Congreso Nacional, a los 15 días del mes de octubre del año 2014.

PROPUESTA DE REFORMA AL REGLAMENTO DE LA LEY DE COMERCIO ELECTRÓNICO.

La Honorable Asamblea Nacional,

Considerando:

Que es deber del Estado procurar el cumplimiento de sus normas constitucionales y por tanto garantizar la inviolabilidad de dichas garantías principalmente en lo que respecta a las libertades constitucionales;

Que en el Reglamento a la Ley de Comercio Electrónico, se estipula la vigencia del envío de mensajes de datos;

Que es necesario regular el envío de estos mensajes a efectos de que en los casos que se determinen, se apliquen sanciones por violentar principalmente el derecho a la intimidad de las personas;

En uso de las facultades previstas en el Art. 120 numeral 6 de la Constitución Política del Ecuador, expide el siguiente:

Expide:

LEY REFORMATORIA AL REGLAMENTO DE LA LEY DE COMERCIO ELECTRÓNICO

Art.- 1.- Sustitúyase el Art. 22 por el siguiente:

Art. 22.- **Envío de mensajes de datos no solicitados.-** El envío periódico de información, publicidad o noticias promocionando productos o servicios de cualquier tipo observará las siguientes disposiciones:

a. Todo mensaje de datos periódico deberá incluir mecanismos de suscripción y desuscripción (sic);
b. Se deberá incluir una nota indicando el derecho del receptor a solicitar se le deje de enviar información no solicitada;
c. Deberá contener información clara del remitente que permita determinar inequívocamente el origen del mensaje de datos;
d. A solicitud del destinatario se deberá eliminar toda información que de él se tenga en bases de datos o en cualquier otra fuente de información empleada para el envío de mensajes de datos periódicos u otros fines no expresamente autorizados por el titular de los datos; y,
e. Inmediatamente de recibido por cualquier medio la solicitud del destinatario para suscribirse del servicio o expresando su deseo de no continuar recibiendo mensajes de datos periódicos, el emisor deberá cesar el envío de los mismos a la dirección electrónica correspondiente.
f. Si con el primer envió del mensaje de datos promocionando productos

y servicios, no se recibiere respuesta favorable del propietario de la cuenta de correo electrónico o del número celular receptor, se prohíbe expresamente el envió de mensajes posteriores.

Las solicitudes de no envío de mensajes de datos periódicos, se harán directamente por parte del titular de la dirección electrónica de destino.

Los proveedores de servicios electrónicos o comunicaciones electrónicas, a solicitud de cualquiera de sus titulares de una dirección electrónica afectado por el envío periódico de datos no solicitados, procederán a notificar al remitente de dichos correos sobre el requerimiento del cese de dichos envíos y de comprobarse que el remitente persiste en enviar mensajes de datos periódicos no solicitados podrá bloquear el acceso del remitente a la dirección electrónica afectada.

Es dado y firmado en la Sala de Sesiones del Honorable Congreso Nacional, a los 15 días del mes de octubre del año 2014.

F. Presidenta de la Asamblea

F. Secretaria de la Asamblea

10. BIBLIOGRAFIA

- ALESTUEY DOBÓN, María del Carmen. "Apuntes sobre la perspectiva criminológica de los delitos informáticos", Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi.
- ÁLVAREZ DE LOS RÍOS, José Luis. "Delitos Informáticos". Ponencia en las Jornadas sobre Marco Legal y Deontológico de la Informática, Mérida 17 de septiembre de 1997.
- Andrade Santander, Diana. El Derecho a la Intimidad, Centro Editorial Andino, Quito – Ecuador, 1998.
- BAÓN RAMÍREZ, Rogelio. "Visión general de la informática en el nuevo Código Penal", en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996.
- baratta alessandro: Derecho Penal Mínimo, Editorial Temis S.A. Santa Fe de Bogotá, Colombia, 1999.
- Barbieri Pablo, Contratos de Empresa, Editorial Universidad, Buenos Aires, Argentina, 1998.
- BARRIUSO RUIZ, Carlos. "Interacción del Derecho y la informática", Dykinson, Madrid, 1996, pág. 245 a 252.
- Beccaria Alessandro, De los Delitos y las Penas, Editorial Temis S.A. Santa Fe de Bogotá, Colombia, 1997.
- BERDUGO GOMEZ DE LA TORRE, Ignacio: Honor y libertad de expresión. Tecnos. Madrid, 1.987.

- Bettiol Giusseppe, Derecho Penal, Editorial Temis, Bogotá, Colombia, 1990
- BUENO ARÚS, Francisco. "El delito informático", Actualidad Informática Aranzadi Nº 11, abril de 1994.
- Cabanellas, Guillermo, Diccionario de Derecho Usual, Tomo 1, Editorial Heliasta. 1990.
- Cano Jeimy, Inseguridad Informática: Un concepto dual de la Seguridad Informática. Universidad UNIANDES 1994
- CASTILLO JIMENEZ, María Cinta, RAMALLO ROMERO, Miguel. El delito informático. Facultad de Derecho de Zaragoza. Congreso sobre Derecho Informático. 22-24 junio 1989.
- CHOCLAN MONTALVO, José Antonio. "Estafa por computación y criminalidad económica vinculada a la informática", Actualidad Penal Nº 47, 22-28 diciembre 1997
- Correa Carlos María, El Derecho Informático en América Latina, Publicado en Derecho y Tecnología Informática, Edit. Temis, Bogotá, Mayo de 1990.
- Creus Carlos, Derecho Penal Parte Especial, Edit. Astrea, Buenos Aires, 1998, Tomo 2.
- Cuervo José, Delitos Informáticos y Protección Penal a la Intimidad, Publicación hecha en Internet URL: www.derecho.org
- Dallaglio Edgardo Jorge, "La Responsabilidad Derivada de la Introducción y Propagación del Virus de las Computadoras", publicado en El Derecho, año 1990.
- Davara Rodríguez, Miguel Angel, Análisis de la Ley de Fraude

Informático, Revista de Derecho de UNAM. 1990.

- DAVARA RODRÍGUEZ, Miguel Ángel. "De las Autopistas de la Información a la Sociedad Virtual", Editorial Aranzadi, 1996.
- DAVARA RODRÍGUEZ, Miguel Ángel. "Manual de Derecho Informático", Editorial Aranzadi, Pamplona, 1997.
- Donoso Abarca, Lorena, análisis del tratamiento de las figuras relativas a la informática tratadas en el título xiii del código penal español de 1995.
- FERNÁNDEZ CALVO, Rafael. "El Tratamiento del llamado "Delito Informático" en el proyecto de Ley Orgánica de Código Penal: Reflexiones y propuestas de la CLI (Comisión de Libertades e Informática), Informática y Derecho Nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996.
- FERREYROS SOTO, Carlos. "Aspectos Metodológicos del Delito Informático", Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996
- Fígoli Pacheco, Andrés. El Acceso No Autorizado a Sistemas Informáticos, Uruguay 1998, Publicación hecha en Internet, www.derecho.org.
- Frosini Vitorio, Informática y Derecho, Editorial Temis, Bogotá, Colombia, 1988.
- Fumis Federico, Informática y Derecho de Daños, Boletín Hispanoamericano de Informática y Derecho, 1998, Buenos Aires, Argentina. URL: Http//ww.ulpiano.com
- GARCÍA GIL, F. Javier. "Código Penal y su Jurisprudencia. Adaptada

a la Ley Orgánica 10/1995, de 23 de noviembre", Editorial Edijus, Zaragoza, 1996.

- García Vitoria, Aurora. El Derecho a la Intimidad en el Derecho Penal y en la Constitución de 1978. Editorial Aranzadi, Pamplona – España, 1983.
- GÓMEZ PERALS, Miguel. "Los Delitos Informáticos en el Derecho Español", Informática y Derecho Nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi.
- GUASTAVINO, Elías P., Responsabilidad Civil y otros problemas jurídicos en computación, Ediciones La Rocca, Buenos Aires, 1987.
- Guibourg Ricardo A., Alende Jorge O., Campanella Elena M., Manual de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires, Argentina.
- Gutiérrez Francés, María Luz, Fraude Informático y estafa.
- GUTIÉRREZ FRANCÉS, Mª Luz. "Fraude informático y estafa", Centro Publicaciones del Ministerio de Justicia, Madrid, 1991.
- Hance Olivier. Leyes y Negocios en Internet. México. De. Mc Graw Hill Sociedad Internet. México. 1996.
- Hanssener Winfried, "Derecho Penal", Editorial Azalea, 1998.
- HEREDERO HIGUERAS, Manuel. "Los Delitos Informáticos en el proyecto de Código Penal de 1994", Informática y Derecho Nº 12, 13, 14 y 15, UNED, Centro Regional de Extremadura, Mérida, 1996.
- HERNÁNDEZ GUERRERO, Francisco. "Delitos Informáticos", Ponencia Jornadas sobre el Marco Legal y Deontológico de la

Informática, Mérida, 17 de septiembre de 1997.

- Huerta Miranda, Marcelo y Líbano Manzur Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur.
- Hulsmann Louk, Derecho Penal, 1982
- Jijena Leiva, Renato, Chile: Protección Penal a la Intimidad y los Delitos Informáticos, Editorial Jurídica de Chile, 1993.
- JOVER PADRÓ, Joseph. "El Código Penal de la informática", X Años de Encuentros sobre Informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi Editorial, Pamplona, 1997.
- Larrea Holguín, Juan, Derecho Civil del Ecuador, Los bienes y la posesión, Tercera Edición, Corporación de Estudios y Publicaciones.
- Lima De La Luz, María. "Delitos Electrónicos" en Criminalia. México. Academia Mexicana de Ciencias Penales. Ed. Porrúa. . No. 1-6. Año L. Enero - Junio 1984.
- Madrid-Malo Garizabal Mario, Derechos fundamentales, Escuela Superior de Administración Pública, Santa Fe de Bogotá – Colombia, 1992.
- Magliona Markovicth Claudio Paúl, López Medel Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999
- MANZANARES, José Luis y CREMADES, Javier. "Comentarios al Código Penal"; La Ley- Actualidad, Las Rozas (Madrid), 1996.
- MERLAT, Máximo, Seguridad Informática: Los Hackers, Buenos Aires Argentina, 1999, Publicación hecha en Internet. www.monografías.com

- Mir Puig Santiago, Función de la Pena y la Teoría del Delito en el Estado Social y Democrático de Derecho, Bosch, 1979
- MORAL TORRES, Anselmo del. “Aspectos sociales y legales de la seguridad informática”, Ponencia 1ª Jornadas sobre “Seguridad en Entornos Informáticos”, Instituto Universitario “General Gutiérrez Mellado”, Madrid 12 de marzo de 1998.
- MORALES PRATS, Fermín. “El Código Penal de 1995 y la protección de los datos personales”, Jornadas sobre el Derecho español de la protección de datos personales, Madrid, 28 al 30 octubre de 1996, Agencia de Protección de Datos, Madrid, 1996, pág. 211 a 250.
- Novoa Monreal Eduardo, Curso de Derecho Penal, 1966, Universidad de Chile.
- Palazzi Pablo Andrés, Virus Informáticos y Responsabilidad Penal, sección doctrina del diario La Ley, 16 de diciembre de 1992. Http://ulpiano.com
- PARELLADA, Carlos Alberto, Daños en la actividad judicial e informática desde la responsabilidad profesional, Ed. Astrea, Buenos Aires, 1990.
- PÉREZ LUÑO, Antonio Enrique. “Ensayos de informática jurídica”, Biblioteca de Ética, Filosofía del Derecho y Política, México, 1996.
- PÉREZ LUÑO, Antonio Enrique. “Manual de informática y derecho”, Editorial Ariel S.A., Barcelona, 1996.
- Pierini Alicia, Lorences Valentín, Tornabene María Inés, Hábeas Data, Derecho a la Intimidad, Editorial Universidad, Buenos Aires – Argentina, 1998.

- Radbruch Gustav, Teoría General del Derecho, 1990
- Reyna Alfaro Luis Miguel, Fundamentos para la protección penal de la información como valor económico de la empresa. Publicación hecha en internet en www.dercho.org.pe.
- Resa Nestares Carlos: Crimen Organizado Transnacional: Definición, Causas Y Consecuencias, Editorial Astrea, 2005.
- Rivera Llano, Abelardo, Dimensiones de la Informática en el Derecho, Ediciones Jurídicas Radar, Bogotá, Colombia. 1995.
- ROMEO CASABONA, Carlos María. "Delitos informáticos de carácter patrimonial", Informática y Derecho Nº 9,10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.
- ROMEO CASABONA, Carlos María. "Los llamados delitos informáticos", Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, 1995.
- ROMEO CASABONA, Carlos María. "Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la información", FUNDESCO, Colección impactos, Madrid, 1987.
- RUIZ VADILLO, Enrique. "Responsabilidad penal en materia de informática", Informática y Derecho Nº 9,10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996.
- RUIZ VADILLO, Enrique. "Tratamiento de la delincuencia informática como una de las expresiones de criminalidad económica", Poder Judicial número especial IX, 1989.
- Salt G. Marcos, Informática y Delito, Publicación en Internet, URL:

http://www.derecho.org.ar

- Santos Jaime Eduardo y Guerrero M María Fernanda. Fraude Informático en el Banca, Ed. Jesma, Bogotá, 1993
- SERRANO GÓMEZ, Alfonso. "Derecho Penal. Parte Especial I. Delitos contra las personas", Dykinson, Madrid, 1996.
- Solano Bárcenas, Orlando, Manual de Informática Jurídica, Editorial Jurídica Gustavo Ibáñez, Santa Fe de Bogotá D.C. Colombia 1997.
- TELLEZ VALDÉS, Julio. "Los Delitos informáticos. Editorial Temis 1999.
- TELLEZ VALDÉS, Julio. "Los Delitos informáticos. Situación en México", Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, pág. 461 474.
- TIEDEMANN, Klauss. "Poder económico y delito", Barcelona, 1985.
- TORTRAS Y BOSCH, Carlos. "El delito informático", número 17 monográfico de ICADE, Revista de las Facultades de Derecho y Ciencias Económicas y Empresariales.
- Velú, Jacques. Convención Europea de Derechos Humanos: El respeto a la Intimidad en el hogar y las comunicaciones. Publicación hecha en Internet www.google.com
- Williams Phil, Crimen Organizado y Cibernético, sinergias, tendencias y respuestas. Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon. http://www.pitt.edu/~rcss/toc.html
- Zabala Baquerizo Jorge, Delitos contra la Propiedad, Tomo 2, Editorial Edino, Guayaquil, Ecuador, 1988.

- Zanoni Leandro. Los Hackers, la nueva cara de los piratas de Fin de siglo, Revista de Informática y Derecho. De Palma, Buenos Aires Argentina 1998.

11. ANEXOS

ENCUESTA

PRIMERA PREGUNTA:

¿Considera usted que es necesario que en nuestro país, se mantenga una actualización constante de la normativa legal en lo referente a la protección de los derechos de las personas en general?

SEGUNDA PREGUNTA:

¿En el mismo sentido de la pregunta anterior, según su criterio cree usted que los derechos de las personas a la intimidad se ven constantemente afectados por acciones realizadas a través del uso del internet?

TERCERA PREGUNTA

¿Según su criterio, el Estado ha cumplido eficazmente con su responsabilidad de frenar la comunicación no solicitada de productos y servicios en el país; a través del internet?

CUARTA PREGUNTA

¿Considera usted que siendo el spam un mensaje de datos no solicitado que atenta al derecho a la intimidad, debe regularse como una conducta delictiva?

QUINTA PREGUNTA:

¿Según su criterio considera usted que el envío de mensajes de datos no solicitados o spam, debe sancionarse también en la Ley de Comercio Electrónico a efectos de frenar esta acción delictiva?

SEXTA PREGUNTA:

¿Considera usted que es necesario que en la ley de Comercio Electrónico y Mensajes de Datos, así como en su reglamento, se regule de debida forma, una sanción administrativa y penal al envío de mensajes de datos no autorizados?

SEPTIMA PREGUNTA

¿En su experiencia considera usted que la norma del Art. 22 del Reglamento a la Ley de Mensaje de Datos impide sanciones eficaces al envio de mensajes de datos?

OCTAVA PREGUNTA

¿Considera usted que es necesario entonces una reforma a varios cuerpos legales, es decir a la Ley de Comercio electrónico pero tambien a su reglamento?

ÍNDICE