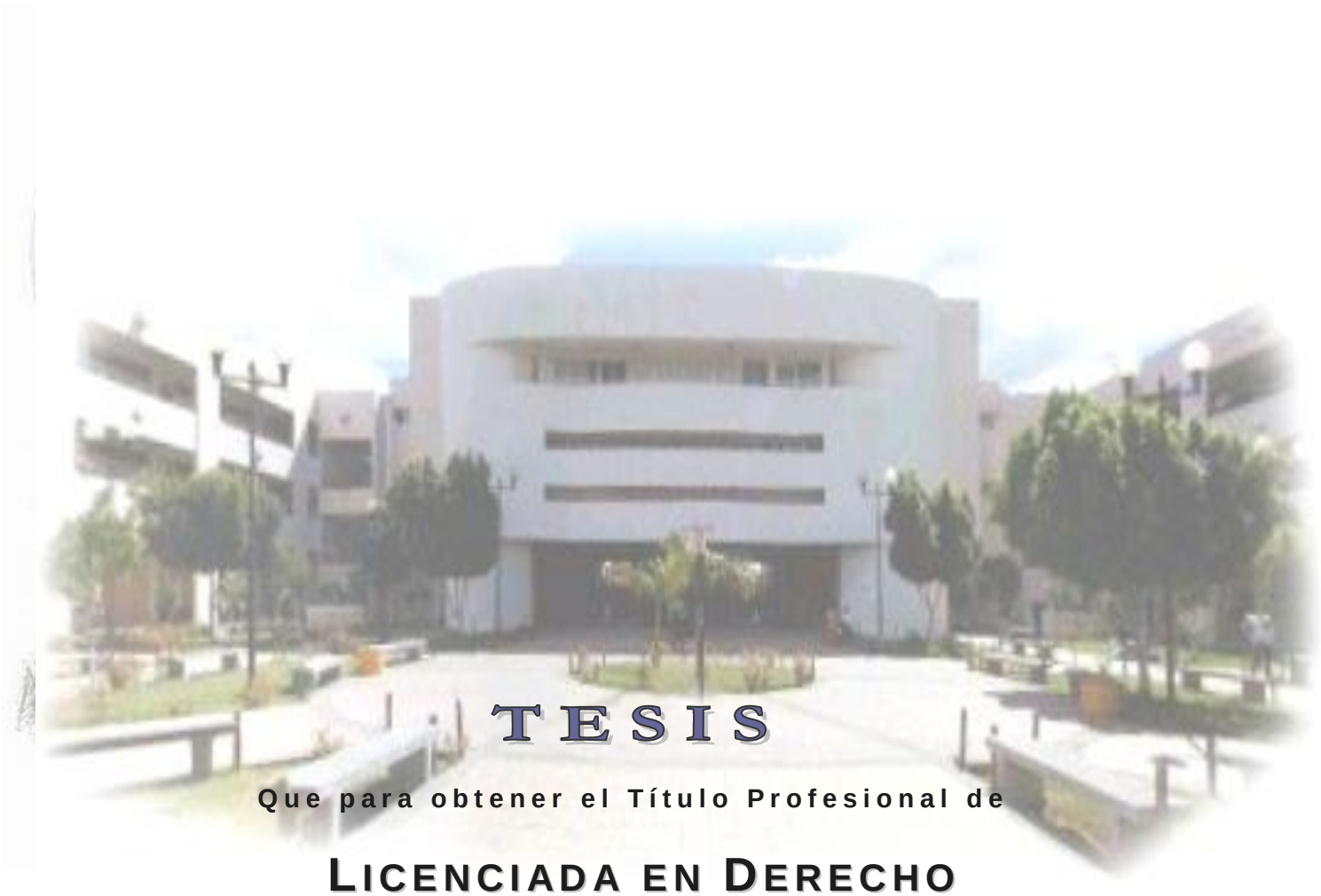
DERECHO INFORMÁTICO



TESIS

Que para obtener el Título Profesional de

LICENCIADA EN DERECHO

Astrid Alicia Verdugo Sánchez

DIRECTORA DE TESIS: Lic. Martha Martínez García

Hermosillo, Sonora. Enero de 2011.

Universidad de Sonora

Repositorio Institucional UNISON

Índice

INTRODUCCIÓN

Los paradigmas de interacción humana actualmente han rebasado aspectos de localidad, concebida esta expresión como aquellas circunstancias en las que los seres humanos se comunican directamente, es decir una persona frente a otra. A través de los esfuerzos históricos por abrazar mayor tiempo y espacio el hombre ha creado tecnología que le ha dados resultados satisfactorios que la ha sofisticado en la reducción de distancias, y tiempos de inversión para lograrlo. Hoy día, a éste ejercicio tecnológico lo ha denominado como: Comunicación a través de Nuevas Tecnologías, Sistemas de comunicación electrónica, Redes Tecnológicas de Comunicación, Sistemas de Internet

Si bien es cierto, que de acuerdo con diversas fuentes de información se reconoce que particularmente la tecnología computacional detonó como un sistema originado en instancias militares, actualmente se utiliza de manera cotidiana para el trabajo gubernamental tanto en la comunicación, control y resguardo de datos, también en la investigación, actividades comerciales y la comunicación de la población en general. En razón de lo anterior, se han creado intereses personales y patrimoniales alrededor del uso de la tecnología de la informática, lo que apertura a la ciencia del derecho para facilitar su uso, tutelar los intereses de personas que se generen con las actividades que se desarrollen a partir de uso de los Sistemas de las Nuevas Tecnologías a partir de un orden jurídico o principios de derecho.

Metodológicamente me avoqué a darme a la tarea de obtener información en diversos en documentos formales e informales, en documentos al papel y digitalizados, criterios científicos generales y comentarios que están en los ciudadanos que usan las nuevas tecnologías computacionales, revisión de teorías del derecho alrededor de ésta temática y normas jurídicas existentes, se generaron en mi interior varios intereses y cuestionamientos de lo encontrado. Lo interesante de conocer la inventiva del ser humano en éste campo, la velocidad con que se ha

desarrollado en los últimos años, la facilidad de reducción de comunicación en tiempo frente a una geografía mundial, la capacidad de realizar grandes cantidades de algunos trabajos que se pueden concentrar en una sola base de datos, la dependencia que actualmente tenemos de las computadoras y el Internet como sociedad para gobernarnos, convivir, realizar quehaceres domésticos, proyectar expectativas. La citada búsqueda de información motivada por la intención de una investigación para obtener mi grado de Licenciatura en Derecho también me llevó a cuestionarme que tanto ha incursionado ésta ciencia para estudiar éste fenómeno social visto como la consecuencia de fácil acceso a la tecnología virtual, considerando lo accesible que es tener computadora e Internet en casa, lugares de trabajo y gobierno. Pues también encontré que a la par hay y actividades sociales secundarias como las bursátiles sin necesidad de salir de casa, gestiones y pagos fiscales; personalísimas como conversaciones, envíos de correos; mercantiles entre personas morales, morales con físicas, entre personas físicas; asimismo, otras de carácter negativo como la comisión de delitos, procesos sociales como obtener información de instancias de gobierno, la publicación de información de éstas mismas instancias hacia la comunidad, otros de tipo muy particular como los sistemas cerrados de intranet usados en empresas o en instituciones. Actividades o procesos sociales todos que obligan a la presencia de un orden normativo jurídico que ofrezca seguridad y tranquilidad para quienes lo usan.

Encontré que estas condiciones que se dan en el contexto internacional tienen efectos en el ámbito local, y que actualmente ya hay problemáticas a resolver por la ciencia del derecho y las instancias jurisdiccionales. Así me propongo revisar a través del método comparado las propuestas teóricos jurídicas que se hayan generado y la implementación de normas jurídicas relacionadas en el derecho positivo.

Considerando que la computadora es un instrumento que en la actualidad la traemos con nosotros como un objeto indispensable por los sistemas de inteligencia con que los han alimentado, decidí iniciar la búsqueda de saber dónde podemos

encontrar el derecho que lo tutela (informático) en la normatividad jurídica mexicana, observando que “El derecho informático está debidamente reconocido en México, pero por estar disperso en múltiples leyes, requiere concentrarse en una legislación específica para su control”. Por lo tanto para comprobarlo recurrí a la investigación documental para conocer hechos históricos, conceptos relacionados, propuestas doctrinarias y revisión del derecho objetivo mexicano relacionado con mi tema central “Derecho informático”.

El proceso de revisión de la información del presente trabajo lo he desarrollado mediante una sistemática que presenta aspectos generales del uso de la Informática partiendo del planteamiento de una situación, su proceso histórico de inserción en las necesidades humanas, la postulación de participación de la ciencia derecho desde su postura teórica como derecho informático, hasta el derecho positivo registrado en el ámbito Internacional y luego nacional. Es decir, una metodología que va de lo general hacia lo particular.

Preciso destacar que fueron dos los motivos que me llevaron a elegir el presente tema; primero de carácter estrictamente personal académico para efecto de obtener el grado de Licenciatura en Derecho; el segundo, revisar desde una circunstancia actual como es que la ciencia jurídica media en la vida de nosotros los humanos a medida que evolucionamos. Mi trabajo a desarrollar lo concentré en revisar el orden jurídico con que actualmente contamos en el derecho mexicano para el uso de computadoras y sus accesorios e Internet por el impacto en la dependencia que hoy día hemos adquirido del uso de estos instrumentos.

Con tal propósito, diseñé la presente tesis en cuatro capítulos: el primero esta estructurado para conocer los antecedentes que le dan motivo a la revisión normativa, un segundo capítulo que plantea las generalidades relacionadas con las actividades en la sociedad de la información, el capítulo tercero dedicado a tratar totalmente la informática desde la perspectiva del derecho y por último el cuarto capítulo que revisa las preocupaciones en el plano internacional, normas de orden

nacional y comparaciones jurídicas desde la normativa existente en diversos países vía ejemplo en la reglamentación informática.

Hoy que vivimos en la era de la información por la gran multiplicidad de nuevas tecnologías, medios electrónicos y accesorios que hacen fácil la comunicación, la consulta de las doctrinas jurídicas, leyes, jurisprudencia, entre otros, nos obliga a reflexionar en la relevancia de considerar que la ciencia del derecho al responder a las nuevas necesidades sociales incluya de manera permanente en el estudio de la informática jurídica desde la perspectiva del derecho informático.

Capítulo 1
ORÍGEN Y EVOLUCIÓN

La necesidad de un orden en las relaciones humanas aparece en el momento en que surgen los grupos y las familias. Es entonces, que el Derecho se convierte en un producto de la organización social entendido así cuanto éste no puede prescindir de su relación con los demás cuando ha alcanzado cierto grado de evolución, así la necesidad de existencia del Derecho, se convierte en una estrategia de orden para que permite armonizar la convivencia humana. No es fácil para una sola persona sobrevivir sin ayuda de los demás aún hoy en día necesitamos de esa relación con nuestros semejantes al igual que un cazador necesitaba de un pescador y un artesano de ellos dos, hoy en día necesitamos del arquitecto y de el doctor al igual que ellos de nosotros. Es gracias a estas relaciones entre nuestros semejantes que surgió la necesidad de una reglamentación para llevar a cabo una mejor convivencia entre los miembros de un mismo grupo.

Por otra parte en ésta reproducción voluminosa de los a través de su historia, con una inventiva que no descansa en busca de obtener satisfactores a condiciones que él mismo se crea entre las muchas invenciones. Particularmente el caso que me ocupa en éste capítulo es el de reseñar como a través de la historia hasta hoy podemos contar con la computadora como un instrumento que facilita algunos quehaceres en nuestra vida y de la que el derecho como ciencia no se ha podido abstraer.

1.1 Creación y evolución de la computadora

En la creatividad de las antiguas civilizaciones griega y romana nació el ábaco como un instrumento mecánico para contar, como un dispositivo con cuentas ensartadas en varillas que a su vez están montadas en un marco rectangular.

Mismos que representaban valores almacenados, posteriormente, fue la Pascalina inventada por Blaise Pascal (1623 - 1662) de Francia y la de Gottfried Wilhelm von Leibniz (1646 - 1716) de Alemania. Con estas máquinas, los datos se representaban mediante las posiciones de los engranajes, y los datos se introducían manualmente estableciendo dichas posiciones finales de las ruedas, de manera similar a como leemos los números en el cuentakilómetros de un automóvil.

1.1.1. Primera generación

La primera computadora fue la ***máquina analítica*** creada por Charles Babbage, profesor matemático de la Universidad de Cambridge en el siglo XIX. La idea que tuvo Charles Babbage sobre un computador nació debido a que la elaboración de las tablas matemáticas era un proceso tedioso y propenso a errores. En 1823 el gobierno Británico lo apoyo para crear el proyecto de una máquina de diferencias, un dispositivo mecánico para efectuar sumas repetidas.

Mientras tanto Charles Jacquard (francés), fabricante de tejidos, había creado un telar que podía reproducir automáticamente patrones de tejidos leyendo la información codificada en patrones de agujeros perforados en tarjetas de papel rígido. Al enterarse de este método Babbage abandonó la máquina de diferencias y se dedico al proyecto de la máquina analítica que se pudiera programar con tarjetas perforadas para efectuar cualquier cálculo con una precisión de 20 dígitos. La tecnología de la época no bastaba para hacer realidad sus ideas.

En 1947 se construyó en la Universidad de Pennsylvania que fue la primera computadora electrónica, el equipo de diseño lo encabezaron los ingenieros John Mauchly y John Eckert. Esta máquina ocupaba todo un sótano pero tenía la capacidad de realizar cinco mil operaciones aritméticas en un segundo, proyecto, auspiciado por el departamento de Defensa de los Estados Unidos cuando se integró a ese equipo el ingeniero y matemático húngaro John Von Neumann (1903 - 1957). que es considerado el padre de las computadoras.

El desarrollo de las computadoras suele registrarse por generaciones según dos criterios que deben cumplirse: La forma en que están construidas y la forma en que el ser humano se comunica con ellas.

Esta generación abarco la década de los cincuenta cuyas máquinas tenían las siguientes características: estaban construidas por medio de tubos de vacío y eran programadas en lenguaje de máquina, son grandes y costosas.

En 1951 aparece la UNIVAC (NIVersAl Computer), fue la primera computadora comercial, que disponía de mil palabras de memoria central y podían leer cintas magnéticas, se utilizó para procesar el censo de 1950 en los Estados Unidos. Utilizaban tarjetas perforadas.

1.1.2. Segunda Generación

Se redujo su tamaño y creció su capacidad de procesamiento. También en esta época se empezó a definir la forma de comunicarse con las computadoras, que recibía el nombre de programación de sistemas. Su característica: Fueron construidas con circuitos de transistores y se programaron en nuevos lenguajes llamados lenguajes de alto nivel. Son de menor costo. Aparecen muchas compañías para su distribución. Sin embargo, el usuario final de la información no tenía contacto directo con las computadoras.

1.1.3. Tercera generación

En el año de 1960, surge la ***tercera generación*** de las computadoras. Se inaugura con la IBM 360 en abril de 1964. Las características de esta generación fueron las siguientes: Su fabricación electrónica esta basada en circuitos integrados y su manejo es por medio de los lenguajes de control de los sistemas operativos.

A mediados de la década de 1970, aparecen en el mercado las computadoras de tamaño mediano, o ***minicomputadoras*** que no son tan costosas pero disponen de gran capacidad de procesamiento.

1.1.4. Cuarta Generación

Aquí aparecen los ***microprocesadores*** que es un gran adelanto de la microelectrónica, son circuitos integrados de alta densidad y con una velocidad impresionante. su uso se extiende al mercado industrial. Aquí nacen las computadoras personales que han adquirido proporciones enormes y que han influido en la sociedad en general sobre la llamada ***"revolución informática"*.**

Entre 1984 y 1987 se vendieron alrededor de 60 millones de computadoras personales, por lo que no queda duda que su impacto y penetración han sido enormes y su presencia era ya ineludible en prácticamente todas las esferas de control gubernamental, militar y de la gran industria.

1.1.5. Quinta Generación

En vista de la acelerada marcha de la microelectrónica, la sociedad industrial se ha dado a la tarea de poner también a esa altura el desarrollo del software y los sistemas con que se manejan las computadoras. Surge la competencia internacional por el dominio del mercado de la computación.

Japón lanzó en 1983 el llamado "programa de la quinta generación de computadoras", con los objetivos explícitos de producir máquinas con innovaciones. Estados Unidos también persigue objetivos semejantes, que pueden resumirse de la siguiente manera: Procesamiento en paralelo mediante arquitecturas y diseños especiales y circuitos de gran velocidad y manejo de lenguaje natural y sistemas de inteligencia artificial.

1.2. Implicaciones de la computadora como herramienta

La computadora incluida como una herramienta común en el devenir de los haceres del hombre ha causado diversas expectativas, como sensaciones de estrés, angustia, esperanza, tranquilidad, temores, dado que su uso lo posiciona como un instrumento participante en la comunicación, organización, guarda y concentrado de información, pero sobretodo porque el mismo hombre le ha dotado

de inteligencia artificial para colaborar en la toma de decisiones, razón por la que Julio Tellez expresa que “los avances tecnológicos han logrado que las computadoras se conviertan en una de las fuerzas más poderosas de la sociedad actual…provocando serios cambios en los individuos, de índole positivos y otros de índole negativo”[1]

Revisando las implicaciones positivas a las que se refiere el autor citado relaciono las siguientes:

- NUEVAS OPORTUNIDADES DE TRABAJO: Ha aumentado considerablemente la oferta de trabajo para quienes tienen conocimientos computacionales.
- MAYOR SATISFACCIÓN EN EL TRABAJO: Los profesionistas pueden descansar en las computadoras el trabajo repetitivo y dedicarse más tiempo al trabajo intelectual.
- AUMENTO EN LA PRODUCTIVIDAD: Generando mejores productos, ofreciendo mejores servicios, eficiencia, evitando desperdicios.
- ECONOMÍA DE TIEMPO: Por la rapidez en el control de información.

Pero también se han identificado implicaciones negativas del uso de ésta tecnología como:

- CONTÍNUA AMENAZA DE DESEMPLEO: Por la sustitución de fuerza de trabajo o en su caso por creación de crisis económicas.
- PROBLEMAS FÍSICOS Y PSICOLÓGICOS: Por la tendencia hacia la despersonalización, sentimientos de frustración, problemas visuales entre otros.
- PROBLEMAS JURÍDICOS: Como son los de seguridad, confidencialidad de la información, robo de programas, comisión de ilícitos entre otros.

1.3. Algunos usos de la computadora en la actualidad

[1] Téllez Valdés, Julio. Investigador Mexicano cuya línea de trabajo se destaca en el derecho informático comenta del poder que tiene la presencia de las computadoras tanto en organizaciones de todos tamaños como en los mismos hogares.

Aun cuando la intención original de la creación de la computadora buscaba la concentración y transferencia de la información, su uso se ha diversificado y sofisticado de acuerdo con los fines de la tarea que se le destine a realizar, por ello se han particularizado sus avances reflejados en numerosos ámbitos algunos ejemplos de ellos son:

- La creación de oficinas ofimáticas para la expedición de boletos, reservaciones hoteleras, rentas de vehículos, etc.
- Administración, con un adecuado control de nóminas, planeación y conducción de estrategias generales, etc.
- Supervisión y control empresarial en la vigilancia de efectividad de los trabajadores o empleados en general.
- Industria, Con el surgimiento de la llamada “robótica”, que ha permitido un aumento en la productividad de las fábricas, reducción de tiempo y costo.
- Bancario, Con sistemas de movimientos bancarios virtuales pago, cobro, autorización, asesorías financieras.
- Salud, Concentración computarizada de expedientes médicos que contienen historiales, pruebas de laboratorios, tratamientos, controles farmacéuticos.
- Hogar, para lograr una adecuada administración del presupuesto familiar.
- Arquitectura e Ingeniería Civil, para obtener apoyo en el mejor diseño y construcción.
- Periodismo, en el servicio de mayor y mejor comunicación de los despachos noticiosos.
- Bibliotecario, para un mejor control.
- Empresas publicitarias, para el desarrollo de nuevas ideas.
- Vías públicas, mejor control de tráfico y disminución de la contaminación ambiental.
- Seguridad pública, para la localización de personas extraviadas, recuperación de vehículos robados.

- Anticipación en el desarrollo de proyectos, como tomar en cuenta las predicciones meteorológicas.
- Educación, planeación e investigación.
- Arte, diversión y entretenimiento, diseños de juegos, álbumes fotográficos, películas profesionales y hogareñas, creación de animaciones, etc.
- Sistemas jurisdiccionales, para crear jurisprudencia reuniendo rápidamente las cinco sentencias a pesar de las distancias.
- Tareas legislativas, apoyo en diversas tareas entre los integrantes bicamarales para lograr acuerdos en la investigación, análisis, creación modificación o derogación de normas jurídicas

Capítulo 2
CONTEXTOS GENERALES DE ORDEN SOCIAL

2.1. ¿Qué es la sociedad de la información?

Representa un profundo cambio en la organización de la sociedad y de la economía que descansa, por una parte, en una infraestructura tecnológica y otra por nuevas formas de producción; lo que algunos han llegado a identificar como paradigma técnico-económico.

Los elementos primarios para identificar a la llamada sociedad de la información son la convergencia de contenidos y tecnologías de la información y la comunicación dada la existencia de una infraestructura tecnológica que permite producir y acceder a grandes volúmenes de información e instrumentar servicios por vía electrónica.

No se puede desconocer su impacto social en virtud de su elevado potencial de promover la integración social a nivel mundial, al reducir la distancia entre personas y aumentar su nivel de información, pero además con la participación de la Organización de la Naciones Unidas (ONU) en coordinación con la Unión Internacional de Comunicación (UIT) en su integración.

Esta Sociedad de la Información es ideada desde el año 2000 y formalmente logra su implementación en la Resolución 56/183 (21 de diciembre de 2001) de la Asamblea General de las Naciones Unidas donde se aprobó la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) en dos fases. La primera se celebró en Ginebra del 10 al 12 de diciembre de 2003, y la segunda tuvo lugar en Túnez del 16 al 18 de noviembre de 2005[2].

[2] "Primera fase, Ginebra: La cumbre" *Cumbre mundial sobre la sociedad de la información: Ginebra 2003-Túnez 2005.* 17 de Enero del 2006. On line. (http://www.itu.int/wsis/basic/about-es.html) [consulta 15 de septiembre de 2007]

2.2. Declaración de principios de la cumbre de la sociedad de la información

El acceso a la información y los conocimientos es un requisito previo para conseguir los Objetivos de Desarrollo del Milenio (ODM), tiene la capacidad de mejorar el nivel de vida de millones de personas en todo el mundo. Además, una mejor comunicación permite solucionar los conflictos y alcanzar la paz mundial.

En el capítulo 6. Entorno Propicio, la declaración 39 del citado documento anota "El estado de derecho, acompañado por un marco de política y reglamentación propicio, transparente, favorable a la competencia, tecnológicamente neutro, predecible y que refleje las realidades nacionales, es insoslayable para construir una Sociedad de la Información centrada en la persona"[3].

2.2.1. Plan de acción

Los representantes de los países participantes que fueron 50 Jefes de Estado crearon compromisos, entre otros el de fomentar un marco político, jurídico y reglamentario propicio, transparente, favorable a la competencia y predecible, que ofrezca los incentivos apropiados para la inversión y el desarrollo comunitario en la Sociedad de la Información.

Se abre así un extenso abanico de posibles aplicaciones a desarrollar en las instituciones jurídicas que permite superar el acceso a la información legal producto de la edición electrónica de los boletines oficiales y la diversificación de los servicios de información legal entre otras múltiples posibilidades.

En al ámbito de los procesos jurídicos está presente la posibilidad de interconexión entre los bancos de datos, la agilización de la expedición de servicios registrales de manera remota, así como la posibilidad de mejorar las relaciones de

---

[3] "Construir la sociedad de la información: Un desafío global para el nuevo milenio" *Cumbre Mundial sobre la Sociedad de la Información: Ginebra 2003-Túnez 2005.*12 de mayo de 2004. On line. (http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-S.doc) [consultada el 24 de Octubre de 2007]

comunicación y participación ciudadana, así como, entre las instituciones, generando las posibilidades de gobierno en línea y la creación de una red ciudadana.

Capítulo 3
EL DERECHO INFORMÁTICO

A las épocas de grandes cambios en la historia de la humanidad, se les han asignado nombres especiales: el renacimiento, la ilustración, revolución industrial. En nuestros días, es de tal importancia poseer, administrar y transmitir información, que toda la humanidad se siente y se seguirá viendo afectada, influida y posiblemente dominada por quienes tienen, administran y transmiten este recurso, razón por la cual a esta época se le han impuesto los calificativos de "sociedad de información" o de "revolución electrónica", éste último debido a la facilidad con que se transmite información por medio de los sistemas modernos basados en dispositivos electrónicos.

Ello obliga a tener una actitud reflexiva, crítica y responsable, ante los nuevos problemas que acarrea la tecnología de la información, que torna necesario que los estudiosos del derecho adopten, desde tal perspectiva jurídica, una conciencia tecnológica y se familiaricen con aspectos científicos e informáticos, y les incorporen los necesarios ordenamientos jurídicos, a fin de ponerlos al servicio al hombre y de una sociedad más justa y eficiente.

Estamos en una sociedad donde las tecnologías de la información han llegado a ser la figura representativa de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se alude reiteradamente a la expresión "sociedad de la información".

3.1. Aspectos conceptuales

El género humano por nuestra naturaleza, somos grupos organizados con relaciones sociales que hemos normado con apoyo en la ciencia del jurídica, por lo tanto, revisando el lenguaje de comunicación que usamos encontré en este tenor que la raíz etimológica proviene de “regere” “dirigere”, es decir, lo recto y que por lo tanto, lleva la idea de guiar o dirigir; por ello a fin de establecer contacto con mi

tema de análisis revisaremos ahora conceptos de derecho discutidos por los juristas con la finalidad de de identificar plenamente al derecho informático para posteriormente acercarnos a las normas vigentes relacionadas con él.

La filosofía kantiana (Kant 1724-1804), conocida también como filosofía crítica, formula el concepto de Derecho en una postura del Derecho Natural, que está representado por intereses sobre la naturaleza humana, valores jurídicos, justicia y bien común que sería el ideal jurídico: "Es el complejo de las condiciones por las cuales el arbitrio de cada uno puede coexistir con el arbitrio de los demás, según una ley universal de libertad".

Del Vecchio, considera que el Derecho es "la coordinación objetiva de las acciones posibles entre varios sujetos, según un principio ético que las determine, excluyendo todo impedimento"

De manera que se puede concluir que el Derecho es el conjunto de principios, preceptos y reglas a las que están sometidas las relaciones humanas en toda sociedad civil, para lo cual los individuos pueden ser compelidos a observar esos preceptos, principios y reglas por la fuerza.

Por otra parte, recurriendo al método de la clasificación han categorizado desde una concepción dualista del Derecho, en Derecho Objetivo y Derecho Subjetivo.

El Derecho Objetivo entendido como el conjunto de normas destinadas a regular la conducta de los individuos en la sociedad, interacciona con el Derecho Subjetivo que tiene la facultad, poder o señorío individual o subjetivo de ser titular y hacer valer determinado derecho. Que valga la pena aclarar que recurrir a la clasificación no separa el derecho subjetivo del objetivo, solo es conveniente utilizarla para comprenderla mejor. Por ello la doctrina imperante argumenta que, no puede hablarse de un derecho objetivo y un derecho subjetivo aisladamente,

aunque esto no quiere decir que a los efectos metodológicos y para el estudio de las disciplinas jurídicas, no sea conveniente tomar a veces al sujeto y a veces el objeto del Derecho, pero sólo como división metodológica. Es simple esta explicación, porque si tomamos en cuenta que el Derecho constituye reglas plasmadas como un conjunto de normas que implican por un lado reglas bilaterales de conducta humana, y por otro lado, poderes basados en tales preceptos y que son atribuidos a una voluntad para proteger intereses de los individuos y grupos sociales, entonces para que exista esa facultad es necesario que ésta se desprenda del derecho objetivo, por lo tanto, sin existir ese derecho objetivamente hablando, entonces no puede desprenderse de éste esa facultad, poder o señorío de hacer valer ese determinado derecho.

Hans Kelsen, jurista, filósofo y político austriaco Profesor de Filosofía del Derecho de la Universidad de Viena desde 1917, también en la Universidad de Ginebra, Universidad de Harvard, luego en la de Berkeley (1942), defendió una visión positivista que él llamó teoría pura del Derecho en la que plantea un análisis del Derecho que excluye al derecho natural. Es decir, “El Derecho es el orden normativo e institucional de la conducta humana en sociedad inspirado en postulados de justicia, cuya base son las relaciones sociales existentes que determinan su contenido y carácter. En otras palabras, es el conjunto de normas que regulan la convivencia social y permiten resolver los conflictos interpersonales”.

FloresGómez en su libro *Introducción al Estudio del Derecho* expresa que “En general se entiende por derecho el conjunto de normas jurídicas, creadas por el poder legislativo para regular la conducta externa de los hombres en la sociedad, y en caso de incumplimiento esta previsto de una sanción judicial.[4]

Para cumplir con la metodología que me he propuesto, he preferido acercarme a esta investigación desde la perspectiva de identificar definiciones que

[4] FloresGómez González, Fernando. *Introducción al estudio del derecho y derecho* civil. México: Porrúa,2004 p.2

faciliten la comprensión de él; por ello, encontré que por derecho informático en la Enciclopedia virtual wikipedia[5] se entiende que es " El conjunto de principios y normas que regulan los efectos jurídicos de la interrelación entre el Derecho y la Informática".

Pero en el diccionario especializado en la ciencia jurídica de Filosofía y Teoría del Derecho e Informática Jurídica publicado en el año 2004, se establece que "Es el conjunto de normas que dentro de un determinado sistema jurídico, regulan los procesos de información"[6]

La presencia de nuevos retos que produzcan efectos jurídicos da oportunidad a los juristas para entrar en análisis construyendo propuestas doctrinarias, así como alternativas de soluciones ofrecidas al legislador para su regulación. Pero para revisar las propuestas de definición de lo que es el derecho informático, citaré primero algunas definiciones de palabras o expresiones relacionadas con el tema para que por deducción nos acerque a la conceptualización del tema central: El Derecho Informático.

Eduardo García Máynez en su obra de Introducción al Derecho publicado por Editorial Porrúa, Define el Derecho como un conjunto de normas, tratase de preceptos imperativo-atributivo, es decir, de reglas que además de imponer deberes, conceden facultades. Es el Conjunto de normas jurídicas declaradas obligatorias por la autoridad, por considerarlas justas a los problemas surgidos de la realidad histórica.[7]

Fernando FloresGómez González como lo dice en su libro Introducción al Estudio del Derecho y Derecho Civil, publicado por la editorial Porrúa en México en

---

5 "Derecho informático" *Enciclopedia libre electrónica wikipedia* . On line. (http://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico) [consulta 7 de septiembre 2007].

6 Pérez Luño, Antonio Enrique, Ramón Luis Soriano Díaz, Carmelo José Gómez Torres. *Diccionario jurídico. Filosofía y Teoría del Derecho e Informática Jurídica*. Granada: Comares, 2004.

7 García Máynez, Eduardo. *Introducción al Estudio Del Derecho.* México: Porrúa, 2004. P.36

el año 2004; El Derecho proviene del vocablo latino Directum, que significa en su primer origen, lo que dirige o es bien dirigido, no apartarse del buen camino, seguir el sendero señalado por la ley. [8]

Efraín Moto Salazar quién estima que la palabra Derecho viene de "directum", vocablo latino que, en su sentido figurado, significa lo que esta conforme a la regla, a la ley; es decir, lo que no se desvía a un lado ni a otro, lo que es recto.[9]

Asimismo, la información es otra palabra relacionada con el tema de derecho informático y Raymond Ruyer en su libro "la cibernética y el origen de la información" publicado en México el año 1984 dice: La información, en el sentido ordinario de la palabra, es la transmisión a un ser consciente de una significación de una noción, por medio de un mensaje mas o menos convencional y por un soporte espacio-temporal: impreso, mensaje telefónico, onda sonora, etc.[10]

El Investigador de la Universidad de Salamanca en España Julio Ostalé García revisa el origen del concepto de la información en su apunte "Notas para el concepto de información semántica" y dice que "la palabra información proviene del latín clásico, donde presumiblemente era de uso común. El término *informatio* es una sustantivación del verbo *informare*, que por ser transitivo encuentra su mayor generalidad en la expresión *aliquid informare*. Esto último significa literalmente dar forma a un objeto."[11]

Por otra parte, en la revista electrónica *Master Magazín*, dedicada precisamente a revisar temas de Informática, contiene el artículo escrito por Ana Cecilia Lancillota quien expresa que "La informática es la ciencia que tiene como objetivo estudiar el

---

8 Floresgomez González, Fernando *Introducción al estudio del derecho y derecho civil.* México: Porrúa, 2004 p.2

9 Moto Salazar, Efraín, Miguel José Moto. *Elementos del derecho.* México: Porrúa, 1996 p.7

10 Ruyer Raymond. *La cibernética y el origen de la información.* México: Colección popular, 1984 p.11

11 Ostalé García, Julio *Notas para el concepto de información semántica.* España: Universidad de Salamanca, 2006 p.3

tratamiento automático de la información a través de la computadora." [12] El diccionario electrónico integrado en el portal de la revista virtual "*MASTERMAGAZINE"* define al Derecho Informático como "Un conjunto de normas positivas referidas al tratamiento automatizado de la información en sus múltiples aspectos[13]

La documentalista María Eliana Jirón de la Escuela de Bibliotecología de la ciudad de Santiago, Chile en su documento "Concepto de estudio de usuarios" dice La información es un recurso relevante en el desarrollo científico y técnico de la sociedad moderna, es el vehículo que transmite el conocimiento, por lo tanto es un elemento esencial para el bienestar y el progreso. La información es necesaria para la toma de decisiones, el acceso y uso de ella ha dividido a los ciudadanos en pobres y ricos en información, unos que no tienen acceso a ella, y otros que tienen a acceso a la información para las toma de decisiones acertadas y satisfactorias.[14]

Siguiendo la definición de Ernesto Villanueva, el derecho a la información es el objeto de estudio del derecho de la información, entendido éste como la "Rama del Derecho Público que tiene por objeto el estudio de normas jurídicas que regulan las relaciones entre Estado, medios y sociedad, así como los alcances y los límites del ejercicio de las libertades de expresión y de información y el derecho a la información a través de cualquier medio".[15]

En el análisis de la especialista Ana Azurmendi, en la actualidad el derecho a la información se considera autónomo y humano, estructurado según un sujeto (todos los hombres), un objeto (hechos, opiniones e ideas que sean de utilidad social), un contenido (facultades de difundir, recibir e investigar) y unos límites (los

---

[12] Lancillota, Ana cecilia. *Revista digital Master Magazín. On line*. "Definición y significado de informática" (http://www.mastermagazine.info/termino/5368.php)

[13] "Definición y significado de derecho informático*" Master Magazín Revista digital líder en informática*. Internet: (http://www.mastermagazine.info/termino/4584.php) [consultada 22 de octubre de 2007]

[14] Jirón Ramírez, María Eliana. *Conceptos de estudios de usuarios.* Chile: Escuela de Bibliotecología, 2001 p.2

[15] Villanueva, Ernesto. *Derecho mexicano de la información*. México: Oxford, 2000, p. 298

que suponga la convivencia con otros derechos humanos, pudiendo estar a veces por encima del derecho a la información) distintos.[16]

La Licenciada Evangelina Flores Preciado, quien estima que el derecho a la información es una rama relativamente reciente, que nace ante la necesidad de reglamentar y organizar el ejercicio de un derecho natural del hombre, reconocido en las normas internacionales y también en las leyes fundamentales de diversos países.[17]

Julio Téllez Valdes en su libro Derecho Informático publicado por la Universidad Autónoma de México en 1991, lo define como "…una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica y como objeto de estudio (Derecho de la información)"[18].

En febrero de 1999 publican en la Revista electrónica Alfa-Redi, el artículo de Víctor Rodríguez Hernández quien cita la definición expresada por el Dr. Héctor Fix Fierro: "La Informática Jurídica debe entenderse como el conjunto de estudios e instrumentos derivados de la aplicación de la informática al derecho o mas precisamente, a los procesos de creación, aplicación y conocimiento del derecho"[19]

El Dr. Antonio Pérez Luño, quién estima el concepto de que es la aplicación de los sistemas informáticos a las distintas esferas del Derecho, pero que debe alcanzar el estudio, análisis y aprovechamiento de los recursos que ofrece la informática al quehacer jurídico.

---

16 Azurmendi, Ana. *Derecho a la información*, *Guía jurídica para profesionales de la comunicación*. Pamplona: Ediciones de la Universidad de Navarra, 2002 p. 30-32.

17 Flores, Evangelina "La evolución del derecho a la información en México" *Realidad Jurídica*. On line. Internet: (http://realidadjuridica.uabc.mx/realidad/contenido-informacion.htm) [Consultado 20 de Octubre del 2007].

18 Téllez Valdes, Julio. *Derecho Informático*. México: Instituto de Investigaciones Jurídicas, 1991. p.13.

19 Víctor Rodríguez Hernández. "La informática jurídica y su papel en el Derecho Mexicano" *Alfa-Redi Revista de Derecho Informático electrónica.* On line. 7 de Febrero del 1999, (http://docente.ucol.mx/daniel_or/public_html/Marcot.doc) [consultada 04 de octubre de 2007]. ISSN 1681-5726

Por lo anterior, es pertinente expresar que el Derecho Informático es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas que brotan de la actividad informática. Se deduce de este concepto que la Informática en general desde este punto de vista es un objeto regulado por el Derecho.

La informática, como uno de los fenómenos mas significativos de los últimos tiempos, según ya hemos visto, deja sentir su incontenible influjo en prácticamente todas las áreas del conocimiento humano, dentro de las cuales el derecho no puede se la excepción, dando lugar a una nueva ínter disciplina conocida como el derecho informático. Aunque difícil de procesar por el variado numero de peculiaridades y muy a pesar de los opuestos puntos de vista que pudiera provocar, podemos decir que el derecho informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento y como objeto de estudio.

3.2. Diferencia entre derecho informático e informática jurídica

Para facilitar la comprensión sobre el Derecho informático, cabe conocer de la diferencia con la informática jurídica ya que su nombre puede crear confusión con mi tema pero el significado entre ambas es muy diferente, es por eso que considero necesario mostrar dicho significado de cada una de ellas para llegar a entender su diferencia y por eso cite las siguientes definiciones:

Julio Téllez Valdes define la Informática Jurídica como "la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la Informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación."[20]

En Julio de 2000 publican en la Revista electrónica Alfa-Redi, el artículo de Yarina Amoroso Fernández quien menciona que "La Informática ha llegado a

[20] Téllez Valdes, Julio. *Derecho informático.* México: Mc. Graw, 1997 p.86

constituirse en infraestructura del quehacer moderno, dado que bases de datos y redes telemáticas captan, procesan inmediatamente y trasmiten a gran velocidad cantidades ilimitadas de información. Por la connotación adquirida por las nuevas tecnologías, se han producido un conjunto de aplicaciones de la Informática en el ámbito del Derecho en que la Informática es instrumento del Derecho lo que se conoce como Informática Jurídica[21].

El Dr. Héctor Ramón Peñaranda Quintero, autor de la obra "*IUSCIBERNÉTICA"* estima que la Informática jurídica constituye un fenómeno-ciencia, que ha logrado penetrar en todos los ámbitos o áreas del conocimiento humano, y siendo el Derecho una ciencia, por cuanto constituye un área del humano saber, reflejándose en un conjunto de conocimientos, pues, no cae en la excepción de ser tratada por la Informática, dando lugar en términos instrumentales a la Informática jurídica, que consiste en una ciencia que forma parte de la Informática, que al ser aplicada sobre el Derecho busca el tratamiento lógico y automático de la información legal.[22]

Tomando en cuenta los conceptos antes mencionados por los diversos autores sobre la informática jurídica y los conceptos de derecho informático mencionados en el tema anterior, podemos concluir que una simple captura y organización computarizada de la información jurídica, no es el Derecho Informático, ya que se requiere de razonar jurídicamente, aplicar la teoría de los sistemas y aplicar la teoría de la información, entre otros conocimientos.

Es importante mencionar que en la reiterada interrelación Derecho-informática, en los términos de un Derecho Informático se contemplan una serie de

---

21 Amoroso Fernández, Yarina. "Sociedad de la información: Contribución de la Informática Jurídica" *Alfa-redi revista virtual de derecho informático.* Julio del 2002. On line. (http://www.alfa-redi.org/rdi-articulo.shtml?x=1483) Cuba No. 048

22 Héctor Ramón Peñaranda Quintero. "La informática jurídica: mecanismo de gestión de la información jurídica" *1er Congreso ONLINE del Observatorio para la CiberSociedad.* On line.

(http://www.cibersociedad.net/congreso/comms/c13penaranda2.htm) [21 de Octubre del 2007].

implicaciones tanto de orden social, económico, técnico, práctico y evidentemente jurídico, suscitadas por el uso de la informática tal y como vemos en líneas subsecuentes. Aunque difícil de conceptualizar por el variado número de peculiaridad y muy a pesar de los opuestos puntos de vista que pudiera provocar, podemos decir que el Derecho Informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática).

En si podemos identificar que la diferencia entre estas dos ramas, debido a que el Derecho informático "es el conjunto de normas jurídicas que se encargan de regular los actos y aspectos de la tecnología informática y su finalidad es evitar quebrantar los derechos fundamentales para mantener el orden de una sociedad" y la Informática Jurídica "es una herramienta tecnológica puesta al servicio del derecho para hacerlo mas eficiente ya que facilita el procedimiento, almacenaje y recuperación de información jurídica".

Para Téllez Valdes el Derecho Informático es una rama de las ciencias jurídicas que contempla a la informática como INSTRUMENTO (informática jurídica) y como objeto de estudio (derecho de la informática).[23]

El concepto anterior, fue justificado desde la perspectiva y el grado de presencia e importancia que la humanidad le hemos dado a las computadoras y su uso. Máquinas que a los seres humanos nos han provisto múltiples beneficios de índole comercial debido a que hoy día podemos realizar éste tipo de actos jurídicos originados en el contexto consuetudinario, pero que hoy día son reconocidos por el legislador autorizando firmas electrónicas para formalizarlos, por lo tanto, también no han permitido reducir tiempos y espacios para que dichos actos se materialicen. Aparatos que facilitan el control de personas como en el caso del manejo de recursos humanos en las empresas. Herramienta que nos permite entrar en

[23] Telles Valdés, Julio "Derecho Informatico" Instituto de Investigaciones Jurídicas serie a: fuentes b) textos y estudios legislativos, núm.75 On line (http://www.bibliojuridica.org/libros/1/313/pl313.htm) México, 1991.

contacto visual con objetos a fin de precisar su identificación, como en el caso de la comercialización de estos. Usamos las computadoras como un medio para atender situaciones de comunicación de diversa índole: grupal e individual, institucional, de relaciones formales, de trabajo, personales, e incluso de tipo emocional.

Expresa el autor en comento: “Los inevitables avances tecnológicos han logrado que las computadoras se convierten en una de las fuerzas más poderosas de la sociedad actual, haciendo posibles su uso, tanto en organizaciones de todos tamaños como en los mismo hogares. Actualmente dichas máquinas constituyen la fuerza motriz de la revolución informática, la cual está provocando serios cambios en los individuos, cambios de índole positivo y otros de índole negativo”.

Como implicaciones positivas, podemos citar: mayor satisfacción en el trabajo, cuando el uso d la computadora permite resolver problemas complejos en menor tiempo y con el menor esfuerzo; Nuevas oportunidades de trabajo, debido a la sofisticación y diversificación de éste instrumento, así como componentes y servicios que requieren para su optimización, que le dan oportunidad laboral a muchas personas; Aumento en la productividad generando grandes ahorros, mejores productos y servicios. Implicaciones negativas como: Problemas físicos visuales y otros; Socioeconómicos, por el desplazamiento laboral que representa menos participación de personas por un mayor rendimiento y menos pago en los centros de trabajo; Problemas jurídicos identificados en el grado de confidencialidad, seguridad de la información, comisión de delitos a través del uso de los sistemas computacionales.

3.3. Características fundamentales del derecho informático

Visto al Derecho Informático como una rama del derecho que si bien es cierto hoy se ha reconocido, aún no se le ha dado la importancia debida, tal vez porque la atención se ha concentrado en los beneficios que su uso cotidiano ha dado que los perjuicios que con su mal uso se han ocasionado, por ello he decidido relacionar algunas características:

Se considera al Derecho Informático como una serie de normas porque la llamada política informática lo identifica como un conjunto de las mismas y regula los actos jurídicos a partir del uso de la computadora y que por ser una rama del derecho "nueva" se encuentra dispersa en los códigos de materias y leyes del ordenamiento jurídico mexicano como es en materia mercantil, penal, derechos de autor y otros.

Se basa en "Principios", porque aquellos estudiosos del tema, jueces, magistrados, y tratadistas difunden información respecto al tema y en los "Actos" ya que la informática es vinculada y provocada por el hombre.

Existiendo la diferencia entre el hombre y las maquinas automatizadas de la información, que estas, están programadas para ser seguras, inteligentes y precisas.

Toma en cuenta los "Hechos informáticos" ocurridos en la actualidad ya que la informática es un fenómeno humano y es por eso que va mejorando tecnológicamente.

Es un instrumento de derecho, de la libertad de expresión y de la protección jurídica que puede darse a los programas de computación.

Forma sus propios criterios sobre el Internet y las consecuencias en el Derecho mexicano y en la perspectiva general por ejemplo: Marcas, Patentes, delitos, compra, venta y derechos de autor en relación a la informática.

3.4. Fuentes de derecho informático[24]

En los últimos años el Derecho Internacional ha tenido gran desarrollo tendiente para algunas concepciones, a la formación de un Derecho Mundial, cumpliendo los Tratados, (en cuyo sentido amplio se incluyen las convenciones entre dos o más Estados, conferencias internacionales, resoluciones,

[24] Barberis, Julio A. Formación del derecho internacional. Editorial Ábaco. Ed. 1994 pág. 49

recomendaciones, comunicados conjuntos entre varios Estados, las sentencias judiciales y arbitrales), una función importante como fuente de Derecho Internacional.

3.4.1. Los Tratados.

Considerando que son reglas de derecho válidas, que se encuentran directamente regida por el derecho de gentes, tendiente a modificar una situación jurídica existente o a definir ciertos conceptos. Pueden ser nulos en tanto no cumplan con las características de ellos.

En la contratación electrónica internacional, salvo las previsiones expresas en la materia específica, y respecto a los Estados firmantes y aquellos que las incorporen a la legislación interna de cada país posteriormente, resultan Fuentes de Derecho subsidiarias, las Convenciones Internacionales referidas a los contratos, las Convenciones emanadas de las conferencias de La Haya.

Más recientemente, de los trabajos de las Naciones Unidas han surgido la Convención sobre la Prescripción en materia de Compraventa Internacional de Mercaderías En el área de los Estados Americanos y desde la OEA, de la labor de Conferencias especializadas en Derecho Internacional Privado (CIDIP), surgen elaboraciones como la Convención de 1994 aprobada en México, relativa a Derecho aplicable a la contratación internacional. De igual forma se han firmado tratado en el área del MERCOSUR.

3.4.2. La costumbre

Como tema es relevante en cuanto a la contratación informática y a los modelos de contratos en especial, dado que en la normativa interna de muchos países no existe regulación específica, o resulta parcial y dispersa, por lo que en la práctica se recurre a modelos de la normativa internacional, como los modelos de CNUDMI o de la Comunidad Europea, fuentes de inspiración además, de la legislación que se viene creando en los diferentes países.

3.4.3. Las técnicas

Las Reglas Técnicas son de gran trascendencia como Fuente en el Derecho Informático, lo cual ha sido tenido en cuenta por las Organizaciones Internacionales mencionadas, y han establecido normas específicas cada vez más precisas, como es el caso de las que refieren a Criptografía, en el tema de Firma Digital, tema al que OCDE ha dedicado una Resolución especial, o las reglas técnicas relativas a cada una de las demás áreas de la tecnología informática.

3.4.4. La jurisprudencia

Que Cumple importante función en el orden internacional, dada la "textura abierta" del lenguaje jurídico, antes mencionada, para precisar conceptos y en la integración de normas consuetudinarias y principios generales para el derecho informático pues en esta etapa de su desarrollo, sin embargo, la Jurisprudencia es considerada por la mayoría de la doctrina en general, una Fuente de vital importancia, dado el escaso desarrollo normativo en la materia, tanto en el Derecho Privado, como en el Público, en el Internacional como en el interno, existiendo ya numerosas sentencias relativas entre otros temas a derechos autorales, dominios, etc.

3.5. Relación del derecho informático con otras ramas del derecho

La rama del Derecho Informático surge de la creciente importancia de regular los actos relacionados con la informática, por una parte y por otra, bajo la perspectiva de que la multidisciplinaridad ofrece un panorama amplio para la observación de ésta situación en estudio, el Derecho informático como una rama incipiente del derecho, interactuando no solo con otras ramas del derecho, sino también con otras disciplinas.

3.5.1. Derecho constitucional

El Derecho Informático tiene una estrecha relación con el Derecho Constitucional, por cuanto a la forma, la estructura y órganos fundamentales del

Estado, es materia constitucional. De allí, que actualmente se debe resaltar que el manejo y forma de controlar la estructura y organización de los órganos del Estado, se lleva a cabo por medio de la Informática, porque con el debido uso que se le den a estos instrumentos informáticos, se llevará una idónea, eficaz y eficiente organización y control de estos entes. Por otra parte, en la nueva sociedad de la información además de concebirse ésta como una garantía constitucional a través de un instrumento en este caso la computadora, se recurre también de manera natural a la necesidad de comunicar expresando ideas libremente siempre y cuando se omita la interferencia en perjuicio de terceros. De lo que se puede desprender una serie de relaciones conexas con otras materias como sería el caso del Derecho Tributario y el Derecho Procesal y otros derechos más.

3.5.2. Derechos humanos

Los Derechos humanos, indispensables para defender los Derechos fundamentales del hombre, tales como el de la vida, el de la igualdad, el respeto moral, vida privada e intimidad que llevan al hombre a ser dignos y por consiguiente a tener dignidad, con lo que permite catalogar a las personas como íntegras, conviviendo en ambiente de respeto, de libertad y haciendo posible sociedades verdaderamente civilizadas. La relación que puede tener el Derecho Informático con los Derechos humanos es muy grande; sin embargo, muy simple y brevemente se puede mencionar la posibilidad de que exista a través del Derecho Informático esa regulación jurídica que apoye el buen funcionamiento de los órganos jurisdiccionales, por ejemplo; es de imaginar, la eficiencia con que se manejarían nuestras leyes, que colaborarían en un alto grado a la celeridad procesal, punto indispensable para defender los Derechos humanos de las personas que se encuentran en las cárceles nacionales, declaradas éstas a nivel internacional, como centros violadores de los Derechos humanos. Entonces, al existir celeridad, habrá posibilidad de evitar la sobrepoblación en las cárceles, factor que ha influido en la constante violación de estos Derechos; por producir esa sobrepoblación, escasez de alimento para los reclusos, así como carencia de medios sanitarios y de higiene mínimos necesarios. También, se pueden mencionar otras relaciones tratadas en

materia de Derechos humanos como lo es la privacidad e intimidad, que podrían ser burladas por utilización ilícita de los medios informáticos.

3.5.3. Derecho penal

La relación pertinente a evidenciar entre el Derecho Informático y el Derecho Penal, es que el segundo interfiere al regular las sanciones para aquellos hechos que se constituyen violación de normas del Derecho con el incorrecto uso de la informática y en consecuencia produciendo una alteración negativa que correspondiera al Derecho Informático, transformando éstos hechos en materia de delito cibernético o informático, es entonces que se podría comenzar a hablar del Derecho Penal Informático.

3.5.4. Propiedad intelectual

La interacción del Derecho informático con el tema de la propiedad intelectual contribuye a lograr un mejor control de éstos temas, por ejemplo el para penalizar los plagios, la piratería y en sí cualquier ilícito en contra de los Derechos de autor o industriales, cuando se están produciendo ilícitos en contra de intereses de terceros y por medio de los instrumentos informáticos.

3.5.5. Derecho público

Es indiscutible la estrecha y tan importante relación que existe entre el Derecho Informático y el Estado; produciendo consecuencias al bien colectivo y general. El Derecho Informático si bien se relaciona a pesar de su autonomía, con otras ramas del Derecho, no es igual tradicionalmente hablando, por cuanto el Derecho Informático es tan amplio que necesariamente penetra en todo, así como la Informática ha penetrado en todos los ámbitos.

3.5.6. Derecho privado

También se puede hacer referencia al Derecho Informático de carácter Privado, ya que existen innumerables situaciones que son de carácter privado, como por ejemplo, el contrato electrónico, el contrato informático, el comercio

electrónico, el documento electrónico, y así un sin número de figuras jurídicas pertenecientes al ámbito particular o privado, donde se permite ese acuerdo de voluntades, clave para determinar la existencia del Derecho Informático Privado.

3.6. Implicaciones negativas en la informática

3.6.1. Consideraciones en los delitos informáticos

Las evidencias manifiestas por la sociedad en el uso de las computadoras son múltiples, mismas que para su exploración en materia de derecho penal considero pertinente examinar directamente las referencias relacionadas con el tema del delito informático.

3.6.1.1. Clasificación de los delitos informáticos

Siura Arregoitia López Investigadora de la facultad de derecho de la Habana en su artículo "*Rasgos Afines de los Llamados Delitos Informáticos"* menciona algunos de los delitos informáticos más comunes que se presenten en la actualidad y que en el ámbito mundial entre los que con frecuencia se repiten son:

Manipulación de los datos de entrada

Esta actitud de comporta como un fraude y es también conocido como sustracción de datos, delito que de esta nueva generación es el más común en este campo computarizado. Este delito no require de conocimientos técnicos de informática y puede utilizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.[25]

Manipulación de programas

Este consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas.[26]

---

[25] Arregoitia López, Siura L, Rasgos afines de los llamados delitos informáticos, Facultad de Derecho. Universidad de La Habana, consultada el día 22 de octubre del 2007, pagina de Internet http://www.buscalegis.ufsc.br/arquivos/rasgos_afines.htm

[26] Ibíd.

Manipulación de datos de salida

Es el caso de manipulación que usualmente se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. En un comienzo este fraude se llevaba a cabo mediante tarjetas bancarias robadas y hoy en día utilizan equipos y programas especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.[27]

Fraude efectuado por manipulación informática

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es la técnica que se reconoce como “Salami” en la que cantidades de dinero muy pequeñas se van sacando repetidamente de una cuenta y se transfieren a otra.[28]

El Fraude informático lo define el autor español Dr. Carlos Romeo Casabona, el fraude informático es la incorrecta utilización del resultado de un procesamiento automatizado de datos, mediante la alteración en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en perjuicio de tercero.[29]

Hurto calificado por transacciones electrónicas de fondos

Hurto que se comete mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o también cuando se viola el empleo de claves secretas. Este es un delito que en la doctrina esta tipificado como fraude informático.[30]

---

[27] Ibíd.
[28] Ibíd.
[29] Romeo Casabona, Carlos María. *Poder Informático y Seguridad Jurídica*. Madrid, España: Fundesco, 1987.
[30] Ibíd.

Delitos de daños aplicados al hardware

El robo de un establecimiento comercial de una o varias computadoras no constituye un delito informático, pero si el daño o sabotaje al hardware que impide la puesta en marcha de un sistema informatizado de diagnostico medico.[31]

Daño al hardware

Este tipo de delito esta basado sobre bienes materiales y no inmateriales. Puede darse un atentado contra la máquina o sus accesorios (discos, cintas, terminales, etc.).[32]

Sabotaje informático

Que según Rodolfo Herrera Bravo, es una acción típica, antijurídica y dolosa destinada a destruir o inutilizar el soporte lógico de un sistema computacional, empleando medios computacionales. Por ejemplo, introduciendo un virus informático[33]

Espionaje informático

Consiste en obtener no autorizadamente datos almacenados en un fichero automatizado, en virtud de lo cual se produce la violación de la reserva o secreto de información de un sistema de tratamiento automatizado de la misma. Por ejemplo, interceptando la información que circula en línea a través de las líneas telefónicas[34]

Según Marcelo Huerta Miranda, el delito de espionaje informático es toda conducta típica, antijurídica y culpable que tiene por finalidad la violación de la

---

31 Ibíd.

32 Ibíd.

33 Herrera Bravo, Rodolfo *Ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología* "Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena" Universidad de Chile, agsoto 1998. http://derechotecnologico.com/estrado/estrado009.html#Rodolfo%20Herrera%20Bravo

34 Ibíd.

reserva u obligación de secreto de la información contenida en un sistema de tratamiento de la información.[35]

Piratería informática

La piratería informática o copia ilegal de obras digitales, que consiste en la reproducción, plagio, distribución, comunicación, transformación, exportación o importación de software, sin autorización, con o sin ánimo de lucro. Por ejemplo, al grabar en el disco duro la copia de un programa sin contar con la licencia de uso respectiva[36]

Interceptación de comunicaciones

Con esta conceptualización de delito informático, podemos observar como una gran cantidad de estos delitos, son los mismos que encontramos tipificados en nuestro ordenamiento jurídico, como: robo, hurto, fraudes, falsificaciones, estafa, sabotaje, etc. Con la particularidad de que muchos de ellos son ejecutados a través de novedosas modalidades. [37]

Acceso no autorizado

Según el Dr. Claudio Líbano Manzur el acceso no autorizado es un delito informático que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o contraseñas, no causando daños inmediatos y tangibles en la víctima, o bien por la mera voluntad de curiosear o divertirse de su autor.[38]

---

[35] Marcelo Huerta Miranda. "Figuras delictivo - informáticos tipificadas en Chile" *Alfa-redi revista virtual de derecho informático.* 20 de Marzo del 2002. On line. (http://www.alfa-redi.org/rdi-articulo.shtml?x=433)

[36] Ibíd.

[37] ARREGOITIA LÓPEZ, Siura L. *Rasgos afines de los llamados delitos informáticos*, Facultad de Derecho. Universidad de La Habana **2002.**

[38] Claudio Libano Manzur. "Los Delitos de Hacking en sus Diversas Manifestaciones" *Alfa-redi revista virtual de derecho informático.* On line. Abril 2000. (http://www.alfa-redi.org/rdi-articulo.shtml?x=453) [consultada 25 de octubre 2007]

3.6.1.2 Elementos de los delitos informáticos

En cuanto a los elementos del delito es posible citar que la teoría del delito ha conceptualizado a éste desde dos perspectivas: La teoría causalista y la finalista, ésta última tiene particular interés para mi tesis, dado que explica al delito en base a que el hombre siempre actúa motivado por una finalidad conducida por el análisis de la intención en la acción del sujeto, toda vez que al realizar la acción se requiere de tener conocimientos mínimos del uso de la computadora, programa o sistema para alcanzar el fin perseguido.

Es decir, los elementos que integran el delito son: LA ACCIÓN, LA TIPICIDAD, LA ANTIJURIDICIDAD Y LA CULPABILIDAD Y PUNIBILIDAD. De tal manera que por ACCIÓN plantea que es la realización de una actividad en base a un fin, dado que está basada en la dirección del comportamiento del autor con una finalidad previa, donde la acción es una conducta humana relacionada con el medio ambiente, dominada por la voluntad, dirigida y encaminada a un resultado, por tanto la " la voluntad no puede concebirse sino como ideación proyectada"; del "querer interno". Valerse de conocimientos computacionales para obtener información, destruirla o alterarla en perjuicio de otro mediante el uso máquinas o herramientas computarizadas.

La tipicidad que consiste en la adecuación de la conducta a un tipo penal. Del universo de hechos ilícitos, el legislador penal, mediante la técnica del tipo legal, selecciona todos aquellos hechos que por la gravedad o la forma de afectación del bien jurídico protegido, considera merecedores de pena. Así, en el derecho positivo se han encuadrado delitos informáticos dirigidos a actividades reprochables penalizándolas, para efecto de un castigo.

La antijuridicidad que consiste en la contradicción de la conducta típica con el ordenamiento jurídico considerado globalmente. De ahí la conveniencia de previamente establecer la acciones cotidianas y permisibles a realizar a través del uso de instrumentos computacionales para hacerlo efectivo en el derecho

informático. Recordando que la antijuridicidad que no es un concepto específicamente penal, sino que corresponde a la teoría general del hecho ilícito. Por esta razón, se considera que el Derecho Penal es eminentemente sancionador y secundariamente constitutivo, así el derecho informático debe recurrir Al derecho penal cuando con actividades cibernéticas se realice una actividad que deba sancionarse.

La culpabilidad consiste en el juicio de reproche al autor por su conducta típica y antijurídica sobre la base de que en las circunstancias concretas en las que se manifestó su conducta le era exigible una conducta distinta conforme a derecho. Por ello es enteramente importante conocer los criterios de valor para determinar la actitud psicológica que impulse al autor para realizar el acto reprobable a través de una máquina computadora.

Es decir, la culpabilidad tiene un vínculo de naturaleza psicológica, que enlaza a su autor con su acto, siendo el dolo y la culpa sus formas de presentación.

José Cuervo Álvarez en su libro de delitos informáticos menciona que en todo delito de los llamados informáticos, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, o a un tercero[39].

En consecuencia de lo anterior, la expresión delito informático se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

[39] Cuervo Álvarez, José. *Delitos Informáticos: Protección pena de la intimidad*. España: Ávila), 1998. p. 3

También como el 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[40] y la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software[41]

3.6.1.3 Posibles sujetos de los delitos informáticos y los métodos utilizados por los delincuentes

De la misma manera que los demás delitos, existe un sujeto activo y otro pasivo, sin embargo, tratándose de éstos elementos, en el primer caso no estamos hablando de delincuentes comunes ya que el mecanismo y medio de acción que utilizan para producir el daño es muy diferente a los que han usado los delincuentes estándares, la mayoría de estos modernos delincuentes realizan conductas muy especiales y estudiadas las cuales son precisadas para llegar a producir sus grandes delitos. Es por eso que en este capitulo menciono los diferentes tipos de conductas antijurídicas que puede manifestar el sujeto activo, ya que es necesario conocerlas para profundizar, prevenir y detener dichas conductas que poco a poco afectan mas a la sociedad

Sujeto Pasivo

En el Caso de Delitos Informáticos el sujeto pasivo es la víctima del delito, es a la persona natural o jurídica sobre quien recae la conducta de acción u omisión que realiza el sujeto activo, estas victimas normalmente usan sistemas automatizados de información, generalmente conectados a otros.

---

[40] Gómez Perals, Miguel. *Informática y Derecho*, UNED, Centro Regional de Extremadura, septiembre 1992, Mérida, 1994, Editorial Aranzadi, p. 481.

[41] Baon 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,

Dichos delitos generalmente no son denunciados a las autoridades competentes y hasta en algunas ocasiones tampoco son descubiertos por el sujeto pasivo y esto es de suma importancia para que se den a conocer, ya que así, se podrá descubrir los diferentes ilícitos que cada vez van cometiendo los delincuentes informáticos, tal vez el no denunciar dichos delitos es la razón de la falta de leyes que protejan a las víctimas, ya que es necesario que las autoridades tengan la preparación para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática.

Sujeto Activo

El sujeto activo hablando de Delitos Informáticos son personas que poseen ciertas características que no presentan el denominador común de los delincuentes, es decir, los sujetos activos conocen el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información delicada.

Vistos los sujetos como objeto de estudio cuando cometen delitos desde la Informática Jurídica, se les ha asignado nombres que los identifican desde la característica del mismo delito que cometan. Cito algunos que son los que operan con mayor frecuencia.

Hacker es una expresión idiomática inglesa cuya traducción literal al español tiene varios significados, siendo el más popular el atribuido a "una persona contratada para un trabajo rutinario" y que por la naturaleza del mismo su trabajo es tedioso, entregado, hasta se podría maniático.

La palabra hacker aplicada en la computación se refiere a la persona que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites. Los hackers tienen "un saludable sentido de

curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas. No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos".[42]

Cracker: Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web en Internet, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas.

Obviamente que antes que llegar a ser un cracker se debe ser un buen hacker. Asimismo se debe mencionar que no todos los hackers se convierten en crackers.[43]

Phreaker: es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos. [44]

Gurus: Son considerados los maestros y los encargados de "formar" a los futuros hackers. Generalmente no están activos pero son identificados y

---

42 Machado. Jorge. "Hackers, crackers, piratas, phreakers, spoofers, delincuentes informáticos". *Perantivirus.* On line. (http://www.perantivirus.com/sosvirus/general/hackers.htm) [consultada el 29 de octubre del 2007].

43 Ibídem

44 Ibídem

reconocidos por la importancia de sus hackeos, de los cuales sólo enseñan las técnicas básicas.[45]

Carding (Tarjeteo), las personas que se ven vinculados al carding, se ven inmersos al estudio de las tarjetas inteligentes (Smart Card), tarjetas magnéticas u tarjetas ópticas, los cuales comprenden la lectura de estos y la duplicación de las mismas.: uso ilegal de tarjetas de crédito.[46]

Lamer o Script-Kiddes, es un término coloquial inglés aplicado a una persona falta de madurez, sociabilidad y habilidades técnicas o inteligencia, un incompetente, por lo general pretenden hacer hacking sin tener conocimientos de informática. Solo de dedican a buscar y descargar programas de hacking para luego ejecutarlos, como resultado de la ejecución de los programas descargados estos pueden terminar colapsando sus sistemas por lo general destrozando su plataforma en la que trabajan.

Son aprendices que presumen de lo que no son, aprovechando los conocimientos del hacker y lo ponen en práctica sin saber. [47]

Phreaking y Foning, son persona con conocimientos en teléfonos modulares (TM) como en teléfonos móviles, se encuentran sumergidos en entendimientos de telecomunicaciones bastante amplios. Por lo general trabajan en el mercado negro de celulares, desbloqueando, clonando o programando nuevamente los celulares robados. [48]

---

45 Hackers". *Ratz89.* On line. (http://daco25.blogspot.com/2007/08/hackers.html) [consultado 29 de Octubre 2007]

46 "Hackers". *Ratz89.* On line. (http://daco25.blogspot.com/2007/08/hackers.html) [consultado 29 de Octubre 2007]

47 Ídem

48 Ídem

Phisher, es la persona que crea sistemas para hacer Phishing. Son delincuentes informáticos que tratan de engañar a personas para obtener información bancaria o personal, con la que puedan hacer fraude de algún tipo.[49]

Trashing "Basureo", obtienen información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos. [50]

Entre los métodos más utilizados por estos delincuentes para desarrollar sus acciones negativas podemos ubicar:

La liberación de Caballos de Troya: Consiste en introducir dentro de un programa una rutina o conjunto de instrucciones, por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (ejemplo, formatear el disco duro, modificar un fichero, sacar un mensaje, etc).[51]

Superzapping: Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador. El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del ordenador y modificarlo, su equivalente en un PC serian las Pctools o el Norton Disk Editor.

Puertas falsas (backdoors): Es una practica acostumbrada en el desarrollo de aplicaciones complejas que los programadores introduzcan interrupciones en la lógica de los programas para chequear la ejecución, producir salidas de control, etc., con objeto de producir un atajo para ir corrigiendo los posibles errores. Lo que ocurre es que en la mayoría de los casos cuando el programa se entrega al usuario

---

49 Ídem

50 Ibídem

51 "Que es y que no es un hacker" *Delincuentes digitales.* On line. (http://www.geocities.com/delincuentes_digitales/anteced.htm) [consultada el 29 de octubre del 2007]

estas rutinas no se eliminan del programa y proveen al hacker de accesos o facilidades en su labor si sabe descubrirlas.

Bombas lógicas: Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruir o modificara la información, o provocara el cuelgue del sistema.

Ataques asincrónicos. Este es quizá el procedimiento mas complicado y del que menos casos se ha tenido conocimiento. Se basa en las características de los grandes sistemas informáticos para recuperarse de las caídas, para ello periódicamente se graban los datos como volcado de memoria, valor de los registros, etc., de una forma periódica, si alguien consiguiera hacer caer el sistema y modificar dichos ficheros en el momento en que se ponga de nuevo el funcionamiento del sistema este continuara con la información facilitada y por tanto la información podría ser modificada o cuando menos provocar errores.

Ingeniera social: Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle el password con alguna excusa convincente.

Recogida de basura (trashing): Este procedimiento consiste en aprovechar la información abandonada en forma de residuo. Existen dos tipos: El físico y el electrónico -El físico se basa principalmente en los papeles abandonados en papeleras y que posteriormente van a la basura. Por ejemplo el papel donde un operario a punto su password y que tiro al memorizarla, listados de pruebas de programas, listados de errores que se desechan una vez corregidos, etc. -El electrónico: Se basa en la exploración de zonas de memoria o disco en las que queda información residual que no fue realmente borrada.

Simulación de identidad: Básicamente en usar un terminal de un sistema en nombre de otro usuario, ya sea por que se conoce su clave, o por que abandono el terminal pero no lo desconecto y ocupamos su lugar. El término también es aplicable al uso de tarjetas de crédito o documentos falsos a nombre de otra persona.

Pinchado de líneas de datos (spoofing): Similar al pinchado de líneas telefónicas, en este caso el objetivo son los sistemas de transmisión de datos (Cable telefónico usado por módem, cableado de una red local, fibra óptica, TV por cable) con el fin de monitorizar la información que pasa por ese punto y obtener información del sistema.

Simulación por ordenador: Se define como el uso de la computadora para simular previamente una situación y de esta forma determinar las acciones a probar. En el contexto del hacking se refiere a la simulación en la computadora propia del sistema a atacar con el fin de elaborar estrategias de acción.

Capítulo 4
NORMATIVAS Y REGULACIÓN

4.1. En el plano internacional

Globalización es un término moderno especialmente usado para describir los cambios en las sociedades y en la economía mundial que resultan de un incremento sustancial del comercio internacional y del intercambio cultural. El término fue utilizado por primera vez en 1985, por Theodore Levitt en su obra la globalización de los mercados (The Globalization of Markets) para describir las transformaciones que venía sufriendo la economía internacional desde mediados de la década de los 60.

Así, los modos de producción y de movimientos de capital se establecen a escala planetaria, mientras los gobiernos pierden atribuciones ante lo que se ha denominado la “sociedad en red”. En éste marco se registra un gran incremento del comercio internacional y de las inversiones debido la interdependencia de las naciones.

En los ámbitos económicos, el término se utiliza para referirse a los efectos que ha producido el comercio internacional, a los flujos de capital, y a los efectos de la liberalización y desregulación del comercio y a las inversiones, esto es lo que suele denominar como “libre comercio”, factor imprescindible en el proceso de globalización.

Este paradigma vigente también permea en las tareas del desarrollo del derecho informático en la comunidad internacional. Recientemente los días 1 al 3 de octubre de 2008, se llevó a cabo en Buenos Aires la Segunda Jornada de Derecho Informático, bajo el tema “Existencia o Ficción del Delito Informático”, cuyo interés se evidenció en las diversas comunidades internacionales, donde se trataron temas de seguridad informática y criminalística, legislación comparada y delitos

específicos, organizaciones internacionales relacionadas, derecho positivo, criterios jurisprudenciales y doctrina jurídica del orden informático.

4.2. Situación en el derecho mexicano.

En el derecho mexicano son localizables las normas jurídicas relacionadas con el derecho informático en las diversas legislaciones según el área de aplicación, por ello las relacionaré a mediante éste criterio. Sin embargo, su abundancia y diversidad en la aplicación del derecho obliga a confinar éstas en diversos códigos, leyes, reglamentos y criterios jurisprudenciales, así localicé acciones relacionadas directamente con la norma jurídica:

4.2.1. Derecho civil

a) Contratos y convenios electrónicos

Lo cierto es que Internet elimina intermediarios en la distribución y por ello el consumidor sale ganando, consiguiendo precios más bajos y accediendo cómodamente desde su hogar a una mayor variedad de productos y servicios a golpe de "click".

Por otro lado, se abren nuevas formas de atención al cliente, desde servicios de atención telefónica, pasando por información a través de e-mail o incluso la posibilidad de ser atendido a través de chat, comunicación instantánea de datos escritos, de audio o video-conferencia simultánea.

4.2.2. Derecho Mercantil

Respecto de los haceres jurídicos de los comerciantes, las tareas que debe regular el derecho son tantas que las instancias legislativas han debido recurrir a la informática jurídica como son la firma electrónica o digital es un conjunto de datos electrónicos que identifican a una persona en concreto. Suelen unirse al documento que se envía por medio telemático, como si de la firma tradicional y manuscrita se

tratara, de esta forma el receptor del mensaje está seguro de quién ha sido el emisor, así como que el mensaje no ha sido alterado o modificado.

La firma electrónica puede utilizarse en el sector privado, para contratación privada por vía electrónica, entre empresa y consumidor (por ejemplo, la compra de un libro o un compacto por Internet) y entre empresas (por ejemplo, realizar un pedido a un distribuidor) o incluso entre los mismos consumidores finales. Por ello quiero citar algunas normas jurídicas pertinentes:

> CCF. Artículo **1803**.- El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:
>
> I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y…
>
> CCF. Artículo **1805**.- Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o a través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.
>
> CCF. Artículo **1811**.- La propuesta y aceptación hechas por telégrafo producen efectos si los contratantes con anterioridad habían estipulado por escrito esta manera de contratar, y si los originales de los respectivos telegramas contienen las firmas de los contratantes y los signos convencionales establecidos entre ellos.
>
> CCF. Artículo **1834 Bis**.- Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesibles para su ulterior consulta.

Del Código de Comercio, en lo referente al Comercio Electrónico y de los Mensajes de Datos:

> Artículo 89.- Las disposiciones de este Título regirán en toda la República Mexicana en asuntos del orden comercial, sin perjuicio de lo dispuesto en los tratados internacionales de los que México sea parte.

Las actividades reguladas por este Título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del Mensaje de Datos en relación con la información documentada en medios no electrónicos y de la Firma Electrónica en relación con la firma autógrafa.

En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código, se deberán tomar en cuenta las siguientes definiciones:

Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.

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

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

En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

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

Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

Prestador de Servicios de Certificación: La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados.

El comercio electrónico es una herramienta del comercio que tiene por objeto realizar las transacciones comerciales de una forma más rápida y oportuna, involucrando tanto a los oferentes como a los demandantes, basándose en un procedimiento, procesamiento y trasmisión de información digitalizada (sistemas, textos, sonidos e imágenes) llevándose a cabo en redes abiertas o cerradas.

> CC. Artículo 18.- En el Registro Público de Comercio se inscriben los actos mercantiles, así como aquellos que se relacionan con los comerciantes y que conforme a la legislación lo requieran.
>
> CC. Artículo 20.- El Registro Público de Comercio operará con un programa informático y con una base de datos central interconectada con las bases de datos de sus oficinas ubicadas en las entidades federativas. Las bases de datos contarán con al menos un respaldo electrónico.

Mediante el programa informático se realizará la captura, almacenamiento, custodia, seguridad, consulta, reproducción, verificación, administración y transmisión de la información registral, que obliga a la conservación de mensajes electrónicos

Las bases de datos del Registro Público de Comercio en las entidades federativas se integrarán con el conjunto de la información incorporada por medio del programa informático de cada inscripción o anotación de los actos mercantiles inscribibles, y la base de datos central con la información que los responsables del Registro incorporen en las bases de datos ubicadas en las entidades federativas.

El programa informático será establecido por la Secretaría. Dicho programa y las bases de datos del Registro Público de Comercio, serán propiedad del Gobierno Federal.

> CC. Artículo 20 bis.- Los responsables de las oficinas del Registro Público de Comercio tendrán las atribuciones siguientes:
>
> V.- Operar el programa informático del sistema registral automatizado en la oficina a su cargo, conforme a lo previsto en este Capítulo, el reglamento respectivo y en los lineamientos que emita la Secretaría;
>
> CC. Artículo 21.- Existirá un folio electrónico por cada comerciante o sociedad…

4.2.3. Derecho fiscal

El empleo de la tecnología en las actividades comerciales ha dado lugar a importantes cambios entre ellos los relacionados con el fisco, ya que el comercio electrónico genera transacciones susceptibles de tributación. Así, se implementa desde la misma norma jurídica el Impuesto especial a las transacciones electrónicas.

Para que el potencial del comercio electrónico pueda alcanzarse, es necesario proponer un sistema fiscal global, en donde se defina con certeza, neutralidad y de manera justa la carga impositiva de este tipo de transacciones comerciales.

Por otra parte, la responsable para su administración utiliza en sus procedimientos de seguimiento de aplicación de impuestos, instrumentos electrónicos y ópticos, a través de la condición permanente de la factura electrónica, mediante el procedimiento que inicia con la presentación de una solicitud en la opción Mi Portal (debe contar con un CIEC) paso a paso llenar la solicitud.

> **CFF. Art 32-D.** El nuevo procedimiento se realizará a través del portal virtual ubicado en www.sat.gob.mx:

4.2.4. Derecho en materia de propiedad intelectual

La Ley de la Propiedad Industrial establece que serán patentables las invenciones que sean nuevas, resultado de una actividad inventiva y susceptible de aplicación industrial. Propiedad Industrial (Marcas y Patentes), lo referente a los derechos de autor de obras digitales, nombres de dominio Vs. Marcas

LF DER AUTOR. Artículo 13.- Los derechos de autor a que se refiere esta Ley se reconocen respecto de las obras de las siguientes ramas:

I…

XI. Programas de cómputo;

LF DER AUTOR. De los Programas de Computación y las Bases de Datos. Art. 101. Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

LF DER AUTOR. Art. 102. Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección mediante registro de patente se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

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

LF DER AUTOR. Art. 111. Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Ciertamente, el derecho de autor como derecho fundamental, posee esta doble condición que se hace más evidente en su desarrollo en la sociedad del conocimiento, pues con el auge de un medio como Internet, los usuarios adquieren sobre la obra derechos de acceso libre, propios de una sociedad democrática que persigue el acceso universal a la cultura para generar conocimientos.

4.2.5. Protección hacia el consumidor

Por otra parte, la Ley Federal de Protección a los Consumidores, relaciona dicha actividad con las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. Art. 76 BIS. Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

Un ejemplo de acción realizado por la Procuraduría Federal del Consumidor como responsables de verificar que ésta norma particularmente de cumpla con este ordenamiento. Es el caso de la publicidad que se depositaba en los correos electrónicos como si fuera de la Compañía Tecel.

La Procuraduría Federal del Consumidor detectó un correo electrónico fraudulento que utiliza el nombre de la empresa Telcel, bajo el título “duplica el saldo de tu Amigo Kit”. Ofrece al usuario la posibilidad de duplicar su saldo con sólo enviar un mensaje de texto al 7373 a la central de promociones de esta empresa indicando en el contenido el número 55 13700684 50. El único requisito para obtener dicha “promoción” es que el usuario tenga como mínimo $60 o más de saldo activo. ¡Tenga cuidado! Si recibe este correo u otro semejante, haga caso omiso, pues se trata de un fraude: lo que buscan los defraudadores es robarle su

saldo, ya que al enviar el mensaje de texto usted está transfiriendo su saldo a otro número de celular.

Por su seguridad, la Procuraduría Federal de Consumidor recomienda confirmar previamente cualquier promoción directamente con la empresa, en el caso de Telcel marcando desde su celular *111 para clientes con contrato, y *264 para Plan Amigo. La llamada es gratuita. También puede consultar el sitio web www.telcel.com[52]

4.2.6. Derecho laboral

En cuanto al Derecho laboral, el trabajo telemático, la políticas de uso de recursos y sistemas informáticos en el trabajo, los despidos de trabajadores por uso inapropiado de sistemas informáticos en la empresa, el monitoreo de comunicaciones electrónicas a los empleados y la confidencialidad de la información, están íntimamente ligados con el tema.

El desarrollo de nuevas tecnologías de la comunicación, junto con la modificación de todos los modos de producción está trayendo consigo cambios muy importantes en lo que tiene que ver con el empleo, con la contratación y las formas que ahora adopta la relación laboral con todas las dimensiones. Así el teletrabajo se convierte en una alternativa cada vez más aceptable que las forma tradicionales de empleo y a la inserción laboral de los jóvenes que buscan conseguir empleo.

4.2.7. Derecho penal

En ésta área del derecho, podemos identificar hechos que recurren a la informática jurídica para cometer crímenes informáticos, con consecuencias de derecho a estudios por el derecho informático como la planeación de delitos, su ejecución, y los hace también la delincuencia organizada. Pero instancias que se

[52] PROFECO. “Correo electrónico falso de Telcel” 28 de marzo de 2008 http://www.profeco.gob.mx/alertas/alertas08/Correo_electronico_%20falso_Telcel.asp

han institucionalizado para utilizando la Informática criminal forense. Así podemos ubicar que hay normatividad en materia de derecho penal:

> CPF. Capitulo Segundo Acceso Ilicitito a Sistemas y Equipos de Informática. Art. 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Actualmente la mayoría de las instituciones publicas o privadas guardan y respaldan la mayor parte o totalidad de su información por medio de bases de datos, las cuales se encuentran altamente protegidas, ya que va de por medio la integridad de toda la información y de las personas involucradas, así como de el éxito de la empresa o institución, ya que la competencia y ética de estas en su mayoría dependen de los secretos estratégicos y confidencialidad del manejo de su información. Por esto es muy importante proteger tal información y castigar severamente a las personas que violen este derecho; para mi este caso es comparable con artículos que traten sobre el.

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

Usando los medios informáticos la integridad y seguridad de la que se ha hablado anteriormente es mas controlada, ya que existen las tecnologías y medios inteligentes que pueden localizar rápida, efectiva y exacta en la localización de las personas “allanadoras”, y el momento en que sucedió y como sucedió

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

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

En este caso es cuando es cuando se presenta la nombrada “manipulación de los datos de entrada” o “sustracción de datos” que es el mas común a lo que se refieren los delitos informáticos ya que no se necesitan conocimientos y puede hacerlo cualquier persona que sepa como utilizar el procesador de datos.

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

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

En este articulo entra la relación de la persona autorizada a accederla sistema con el nombrado “Cracker” ya Son personas que se introducen en sistemas remotos con la intención de destruir datos es aquí cuando una persona autorizada toma el papel de cracker.

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

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

En este articulo se pueden tipificar varios delitos como “Fraude efectuado por manipulación informática” este se encontraría en el caso de que se utilizara la

técnica “salami” que es cuando por medio del acceso a un sistema pasa cantidades pequeñas repetidamente de una cuenta bancaria y se transfiere a otra, por ser cantidades tan pequeñas “la persona pasiva” no nota el fraude que se ha cometido en ella.

> **CPF. Art.211 bis 5.** Al que estando autorizado para acceder a sistemas y equipo s de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
>
> Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
>
> Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

La mayor de la ocasiones ocurre este delito es por personas que conocen el sistema del grupo financiero al que trabajan como tal se anuncio en el la pagina de Internet de delitos informáticos.

> **CPF. Art.211 bis 6**. Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.

Sólo el juez y el personal autorizado por la PGR y por el director general del Cisen tendrán acceso al sistema electrónico, para preservar la confidencialidad de la indagatoria.

El 21 de agosto siguiente, el ministro Guillermo Ortiz Mayagoitia, que simultáneamente preside la Suprema Corte de Justicia de la Nación y el Consejo de la Judicatura Federal suscribió el Acuerdo Nacional para la Seguridad , la Justicia y la Legalidad , en cuyo compromiso número 35 dicho consejo se obligó a establecer

tales juzgados, “con residencia en el Distrito Federal, que estarán facultados para emitir órdenes de cateo, órdenes de arraigo y autorizaciones para la intervención de comunicaciones, con tecnología informática que les permita proteger la confidencialidad y dar respuesta oportuna a este tipo de solicitudes en todo el país”.

4.2.8. Derecho procesal

La vinculación entre esta área del derecho y el informático se denota a través de la administración de pruebas en soportes informáticos o tecnológicos, desahogo de las mismas, su valoración. Así también como los mecanismos de investigación y obtención de evidencias electrónicas y los peritajes electrónicos

CFPC. CAPITULO IX. Valuación de la prueba. Art. 210-A. Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.

Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta." [53]

[53] “Código Federal de Procedimientos Civiles” *Cámara de diputados H. Congreso de la Unión.* On line. (www.diputados.gob.mx/LeyesBiblio/pdf/6.pdf) [consultado 13 de septiembre del 2007].

Podemos identificar que el artículo anterior regula de forma flexible los medios electrónicos como medios de pruebas con los que las partes pueden proteger sus relativas posiciones, unos de estos medios en el proceso pueden ser el correo electrónico, comprobantes digitales, los discos magnéticos u ópticos, estas pruebas electrónicas pueden encontrarse relacionadas con la regulación de la prueba documental ya que el fin del documento ha evolucionado de tal forma que ha superado el significado tradicional del escrito, esto es con la finalidad de adaptarnos a los nuevos medios probatorios proporcionados por la aplicación de nuevas tecnologías para la representación de la realidad, existen argumentos a favor de la necesidad de admitir la prueba electrónica en procesos de diferentes materias del derecho:

4.2.9. Derecho bancario y financiero

Comprende y facilita este derecho a sus usuarios la convivencia través de la presencia y participación de instituciones bancarias con sus usuarios implementando agilidad de gestión y control con programas electrónicos específicos como el comercio electrónico, publicación y consulta de información, prestación de servicios a través de medios electrónicos y otras tecnologías, interrelación con otras instituciones de crédito, transferencias electrónicas de fondos e Intercambio electrónico de datos entre otros.

> LEY DE INST. DE CRÉDITO. TITULO TERCERO DE LAS OPERACIONES. CAPITULO I. DE LAS REGLAS GENERALES. Art. 52. Las instituciones de crédito podarán pactar la celebración de sus operaciones y la prestación de servicios con el público, mediante el uso de equipos y sistemas automatizados, estableciendo en los contratos respectivos las bases para determinar lo siguiente:
>
> I. Las Operaciones Y Servicios Cuya Prestación Se Pacte;
>
> II. Los medios de identificación del usuario y las responsabilidades correspondientes a su uso, y

III. Los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.

El uso de los medios de identificación que se establezcan conforme a lo previsto por este artículo, en sustitución de la firma autógrafa, producirá los mismos efectos que las leyes otorgan a los documentos correspondientes y, en consecuencia, tendrán el mismo valor probatorio.

4.2.10. Derecho administrativo

La informática es una herramienta ampliamente aprovechada por el gobierno, cumple una función muy útil en la organización y control de miles de procesos administrativos, pero también es usada con creatividad para el desarrollo de proyectos que tienen gran impacto en la sociedad. Por ello cuenta con reglas propias del derecho informático en leyes como: Ley Federal de Procedimientos Administrativos, Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, Ley de Obras Públicas y Servicios Relacionados, Ley Federal de Trasparencia y Acceso a la Información Pública Gubernamental, así como de Tribunales virtuales.

Un acceso, directo o derivado, a de todas las páginas Web del estado en cuestión, principalmente de la mayoría de los organismos u oficinas que tienen que ver en el mismo con la atención de las necesidades ciudadanas. Para facilitar la ubicación y acceso a estas entidades a través de Internet, sus Sitios Web están organizadas por temas, departamentos y por estructura del poder público. Lo anterior significa que los ciudadanos no necesitan conocer o memorizar las direcciones Internet de las distintas entidades del Estado con presencia en la Red para acceder a su información y servicios, sino que, con tan sólo ingresar al portal principal, podrán tener acceso virtual a todas ellas.

Adicionalmente, cientos de procesos y trámites administrativos, implícitos en las transacciones propias de las licitaciones gubernamentales, han sido

simplificados y, con ello, se ha ganado un importante ahorro de recursos y tiempo, como resultado de la implementación de este esquema.

4.2.11. Medios alternos de resolución de controversias

Las nuevas tecnologías abren un campo inédito para el desarrollo de la resolución alternativa de conflictos. Los profesionales dedicados a estas tareas se ven obligados a capacitarse en nuevas técnicas, si quieren ser partícipes del nuevo mundo de la mediación on line. Así encuentra su presencia hoy día la Mediación electrónica y el Arbitraje electrónico, como ejemplo de ello.

A diferencia de la experiencia norteamericana, donde los servicios de mediación on line operan generalmente desde las residencias particulares de los involucrados (clientes y mediadores) utilizando el e-mail, la propuesta del Centro Virtual de Prevención y Resolución de Conflictos prioriza la seguridad y confidencialidad de los datos, amparándose en lo que llaman un sistema institucional.

Cabe mencionar que particularmente en el derecho mexicano no encontré normas jurídicas específicas; aun cuando éste ya que se trabaja, sin embargo tiene tendencias a formalizarse también como un derecho incipiente.

4.3. Algunas jurisprudencias en el ámbito del Derecho informático

El derecho informático como parte de la evolución que ha provocado el hombre de las nuevas tecnologías, y que hemos acordado previamente ha generado nuevas formas de interactuar a partir de ellas, finalmente también se ha involucrado en la complejidad del respeto del derechos de los demás. Por otra parte, desde de la doctrina jurídica y el derecho positivo se ha perfilado como organizador y regulador de los deberes que a cada uno atañen, y por ello que al modificar estructuras de convivencia también se modifican dichas normativas. Sin embargo, dar tiempo a espacios de cambios y análisis desde la postura legislativa, requiere de espacios temporales bastante amplios y la tecnología avanza a

velocidades desfasadas; en ese sentido, es que el derecho ha recurrido a resolver situaciones de esta naturaleza desde la jurisprudencia que emite la Suprema Corte de Justicia de la Nación y sus Tribunales Colegiados de circuito, que tiene como básica tarea la de precisar los aspectos y alcances de una norma legal que el legislador no previó.

PRUEBA DE INSPECCIÓN PRACTICADA ANTE LA PANTALLA DEL SISTEMA INTEGRAL DE DERECHOS Y OBLIGACIONES DEL INSTITUTO MEXICANO DEL SEGURO SOCIAL (SINDO). ES INSUFICIENTE POR SÍ SOLA PARA DEMOSTRAR QUE EL TRABAJADOR NO TIENE EL CARÁCTER DE ASEGURADO DE DICHO ORGANISMO, PUES PARA ELLO DEBERÁ COMPLEMENTARSE CON UNA PERICIAL EN INFORMÁTICA JURÍDICA DOCUMENTARIA.

El Sistema Integral de Derechos y Obligaciones del Instituto Mexicano del Seguro Social (Sindo), es una base de datos contenida en un sistema informático que cuenta con un mecanismo de consulta, a través del cual se puede obtener información sobre si alguna persona es o no asegurado del Instituto Mexicano del Seguro Social. Por otra parte, de los artículos 827 a 829 de la Ley Federal del Trabajo se advierte que la prueba de inspección debe versar sobre documentos u objetos que obren en poder de alguna de las partes, quien deberá ponerlos a la vista del actuario, por lo que su desahogo es únicamente descriptivo. Asimismo, los numerales 821 a 823 de la citada ley reglamentan la prueba pericial, la cual siempre versará respecto de alguna ciencia, arte o técnica de la que los peritos tienen conocimiento o autorización para su ejercicio conforme a la ley. Finalmente, el diverso numeral 776 del aludido ordenamiento regula los medios de prueba que pueden ofrecerse en el procedimiento laboral, entre los que se encuentran los aportados por los descubrimientos de la ciencia, entre los que debe considerarse la informática. Por consiguiente, la prueba pericial en informática jurídica documentaria sobre la referida base de datos será la que asegure el acceso correcto al "Sindo", ya que el perito es quien, con los conocimientos técnicos apropiados, asegurará que la consulta se hizo correctamente, lo cual significa, que los resultados serán confiables y susceptibles de valoración. En tal virtud, la

inspección realizada ante la pantalla del "Sindo", por sí sola, no tiene el alcance de establecer que el solicitante no es asegurado de dicho instituto, ya que el fedatario público describirá sólo lo que la oferente le ponga a la vista, pero de manera alguna puede asegurar que el acceso y la búsqueda hayan sido los que corresponden con la técnica de ese sistema. En suma, para demostrar el supuesto de que se trata, la prueba de inspección es insuficiente por sí sola para acreditar tal extremo, por lo que deberá complementarse con una pericial en informática jurídica documentaria, sin perjuicio de que la institución conserve la confidencialidad y el control de las claves de acceso al sistema, y de que a través de otros medios pueda demostrarse ese hecho.

PRIMER TRIBUNAL COLEGIADO DEL DÉCIMO NOVENO CIRCUITO.

Amparo directo 24/2006. Instituto Mexicano del Seguro Social. 20 de septiembre de 2006. Unanimidad de votos. Ponente: Miguel Mendoza Montes. Secretaria: Piedad del Carmen Hernández Ávila.

SISTEMA COMPUTARIZADO PARA EL REGISTRO ÚNICO DE PROFESIONALES DEL DERECHO ANTE LOS TRIBUNALES DE CIRCUITO Y JUZGADOS DE DISTRITO. PARA TENER RECONOCIDO EL CARÁCTER DE AUTORIZADO EN TÉRMINOS DEL ARTÍCULO 27 DE LA LEY DE AMPARO, EL ABOGADO DEBE ACREDITAR SU INSCRIPCIÓN, PREVIO A LA PROMOCIÓN DE ALGÚN MEDIO DE DEFENSA.

El sistema informático establecido por el Consejo de la Judicatura Federal en el Acuerdo General 24/2005, publicado en el Diario Oficial de la Federación el 18 de julio de 2005, tiene por objeto que efectuada la inscripción de la cédula de licenciados en derecho ante los órganos jurisdiccionales del Poder Judicial de la Federación, surta sus efectos; sin embargo, requiere para su efectividad que el profesional autorizado en términos amplios del segundo párrafo del artículo 27 de la Ley de Amparo, haya registrado los datos de su cédula con fecha anterior a aquella en que intente hacer valer en beneficio de su autorizante algún medio de defensa establecido por la citada ley. Por ello, si de la consulta a dicho sistema se acredita que el registro se efectuó con posterioridad a la promoción, resulta evidente que al momento de presentar el medio de defensa carecía de legitimación en el

procedimiento, atento a que este presupuesto procesal debió estar previamente acreditado porque no puede ser convalidado.

DÉCIMO PRIMER TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL PRIMER CIRCUITO.
Amparo en revisión 275/2005. Gerardo Pilgram Cortina. 25 de noviembre de 2005. Unanimidad de votos. Ponente: Guadalupe Ramírez Chávez. Secretaria: María Guadalupe Casillas Quintero.

Nota: El Acuerdo General 24/2005 citado, también aparece publicado en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XXII, julio de 2005, página 1599.

TRANSFERENCIA ELECTRÓNICA DE FONDOS. CARGA DE LA PRUEBA SOBRE LA AUTORIZACIÓN DE OPERACIONES.

La transferencia electrónica es un instrumento de pago mediante el movimiento de fondos consistente en el cargo que recibe la cuenta del ordenante y el abono que se produce en la cuenta del beneficiario. En la utilización de ese medio de pago, es necesaria la intervención de uno o varios bancos, según se trate de una operación entre cuentas de una misma institución de banca múltiple o interbancaria, de tal suerte que los bancos actuarán como expedidores, intermediarios o receptores de los fondos, e incluso, con todas esas funciones a la vez, para el supuesto de traspasos entre cuentahabientes de una misma entidad bancaria. Sin embargo, para que los bancos actúen en esa cadena de relaciones, es indispensable que exista un iniciador de tal secuencia, o sea, un cuentahabiente ordenante, y un destinatario final que concluya el enlace de nexos, esto es, un cuentahabiente beneficiario. En efecto, las operaciones de transferencia electrónica de fondos, entre ellas las destinadas para el pago de los impuestos federales, son realizadas por los propios depositantes, a través de una institución crediticia, quien a su vez utilizará el servicio prestado por la cámara de compensación respectiva en caso de operaciones interbancarias. Dada esa particular mecánica, es menester acreditar,

en caso de una transferencia cuyo importe no se acepta como cargo a la cuenta de la parte ordenante de la operación, que dicha operación fue realizada directamente por la institución de crédito, incumpliendo así su obligación de abstenerse de realizar retiros que sólo puede hacer la parte depositante. Empero, debe considerarse que la transferencia de fondos se realiza en forma electrónica, de tal suerte que es el sistema computacional del contribuyente el que se enlaza con el sistema del banco, y en ambos sistemas informáticos quedan registradas las operaciones de envío de la instrucción y recepción de la misma, lo que permite al cuentahabiente obtener un comprobante de la operación, pero también el sistema de la institución bancaria registrará de manera automática, como corresponde a los programas informáticos operados por computadoras, la autorización, asignándole un número, con fecha, monto, origen y destino. Lo anterior, genera que sea el banco quien tenga mayores elementos para acreditar no sólo la realización de las operaciones de transferencias electrónicas de fondos, sino también las autorizaciones correspondientes a cada una de ellas, ya que únicamente con base en la orden recibida por el sistema **informático** de la institución de crédito se puede realizar el traspaso automatizado de capitales. De hecho, en todas las operaciones de pagos a terceros, como proveedores de bienes y servicios, realizadas por los cuentahabientes de las instituciones de crédito, es necesario que éstas lleven un registro de las autorizaciones efectuadas por sus clientes, como prevé el artículo 57 de la Ley de Instituciones de Crédito. Por ende, cuando el ordenante de la transferencia niega haber dado una autorización al banco del cual es cuentahabiente para que se hiciera esa operación, y la institución bancaria afirma que sí recibió la instrucción correspondiente, corresponde la carga probatoria a esta última, tanto por ser quien conserva un registro de operaciones que, inclusive, reflejará en los estados de cuenta que tiene que remitir a sus cuentahabientes, como por la circunstancia de que así se desprende de la asignación de las cargas probatorias en cuanto a las afirmaciones y negaciones de hechos establecida en los artículos 1194 y 1195 del Código de Comercio. Así, por regla general, la carga de la prueba sobre la existencia de la autorización para efectuar una transferencia electrónica de fondos corresponde a la institución bancaria, sin embargo, cuando el

cuentahabiente afirma que el banco duplicó el traspaso por un error atribuible al mismo, a pesar de existir el registro de dos autorizaciones distintas, toca al propio cuentahabiente demostrar que fue el banco quien se apartó de la forma de operar un pago a terceros, y en particular una transferencia electrónica, para lo cual podrá exigir no sólo la aportación de los registros del banco sino, inclusive, ofrecer la prueba pericial en informática, entre otros medios de comprobación a su alcance.

TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO. Amparo directo 495/2005. Banco Santander Mexicano, S.A., Institución de Banca Múltiple, Grupo Financiero Santander Mexicano. 18 de agosto de 2005. Unanimidad de votos. Ponente: Neófito López Ramos. Secretario: Raúl Alfaro Telpalo.

4.4. Ejercicios de derecho comparado

Desde el ejercicio del derecho comparado, resulta interesante observar que los Estados Internacionales se preocupan por legislar en materia de derecho informático consignando penas que intimiden como forma de control para aquellos que tengan intención de usar en perjuicio de otro sus conocimientos de computación.

MATERIA: Penal

TEMA: Modificar o Destruir

MEXICO	**VENEZUELA**	**PERU**	**ESPAÑA**
Código Penal Federal Mexicano	Ley contra delitos informáticos.	Código Penal de Perú.	Código Penal español.
Acceso ilícito a sistemas y equipos de informática. Art. 211 bis1,2,3,4,5,6,7	De los delitos informáticos Art. 6-12	Delitos informáticos 207ª,b y c	Delitos informáticos 197
Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de	Artículo 7. Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el	Artículo 207-B.- Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras	2.- Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de

informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.	funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.	El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.	carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. Será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Comentarios:

En la acción de "destruir o Modificar" en materia penal observamos que los cuatro países que estoy comparando reglamentan el mismo delito, presentando algunas diferencias, como:

- Que Perú tiene menos artículos referentes a delitos informáticos, en cambio, Venezuela dedica un código específico para los delitos informáticos.

- Los artículos redactados con mayor similitud son los de Venezuela y México.
- España no tiene articulo que mencione la palabra "Destruir" pero interpretando adecuadamente su articulo 197 apartado 2, podemos apreciar que en la palabra "modificar" infiere el delito de destruir ya que al destruir un dato en un sistema lo esta modificando.

- La penalidad más severa es la de Venezuela que es de cuatro a ocho años y la más menos severa es la de México ya que solo es de seis meses a dos años de prisión.

- La multa más elevada la impone España catalogada de doce a veinticinco meses y la más barata es la de Perú de setenta a noventa días.

TEMA: Seguridad Nacional o del Estado

MATERIA: Penal

MÉXICO	**VENEZUELA**	**PERÚ**
Código Penal Federal	Ley contra delitos informáticos.	Código Penal de Perú.
211 BIS 2	Articulo 11	
Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.	Artículo 11. Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias. La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro. El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.	Artículo 207-B.- Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa. Artículo 207-C.- Delito informático agravado En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo. 2. El agente pone en peligro la seguridad nacional." (*) (*) Capítulo incorporado por el Artículo Único de la Ley Nº 27309, publicado el 17-07-2000.

Comentarios:

- Primero explico que utilicé la comparación “seguridad nacional o del estado” porque son las expresiones registradas por México y Venezuela, en cambio Perú, anota la expresión Estado en el mismo sentido.

- El caso de México prohíbe solamente conocer o copiar información contenida en equipos del estado, en cambio, los otros dos estados contienen similitudes debido a que señalan que la multa aumentara si se pone en peligro la SEGURIDAD del estado.

- España no se refiere en su normatividad indicaciones específicas referentes al derecho informático a la nación o estado, así que el artículo 197 se hace responsable de regular a quienes comentan delitos a sistemas del estado aun poniendo en peligro a la nación.

MATERIA: Penal

TEMA: Personas encargadas o autorizadas

MÉXICO	**VENEZUELA**	**PERÚ**	**ESPAÑA**
Artículo 211 bis 3	**Título III Disposiciones comunes:** Artículo 27	Artículo 207-B	Artículo 198.
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.	Agravantes. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad: 1º Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido. 2º Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función.	Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa. Artículo 207-C.- Delito informático agravado En los casos de los Artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando: 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.	La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Comentario:

Encontré en este tema de “personas encargadas y autorizadas” diferencias entre las legislaciones de los cuatro países que a continuación relaciono:

- El Código Penal Mexicano se refiere únicamente a las personas autorizadas como aquellas destinadas para acceder a sistemas y equipos del estado y no solo se refiere a modificación y destrucción si no también a copiar la información y diferentes penas y multas.

- En la ley contra los delitos informáticos de Venezuela hace referencia sobre las personas encargadas a acceder a un sistema en sus últimos capítulos que se encuentran en las disposiciones comunes y hace general las personas encargadas tanto del estado como las de cualquier otro propietario.

- En el código penal de Perú toma el mismo articulo antes observado en su apartado "C" imponiendo aparte de la multa una pena privativa de libertad para las personas que abusen de su cargo para acceder a equipos ajenos mas no únicamente se refiere a los del estado.

- En el código Penal Español se refiere a autoridad o funcionario publico y no solo lo sancionara con la multa prevista si no que será inhabilitado absolutamente.

Datos comparativos por país del uso de máquinas que cuentan con algún sistema computacional.

	México	Argentina	Chile	Cuba	Perú	Venezuela	Panamá
Población (millones)	106.147	39.53	16,267	11,367	27.947	26,577	3,228
Producto nacional bruto por habitante	6.328	4,728	4.731	1.518	2.843	3.788	4.217
Índice de desarrollo humano	0,814	0.869	0,854	0,817	0,762	0,772	0,804
Aparatos de TV cada 1.000 personas	283	293	242	250	148	185	194
Aparatos de radio cada 1.000 personas	330	681	354	353	273	294	300
Teléfonos fijos cada 1.000 personas	17,22	22,76	21,53	6,78	7,49	12,78	11,85
Teléfonos celulares cada 1.000 personas	36,64	34,76	62,08	0,67	14,85	32,17	26,98
Computadores personales cada 1.000 personas	10,68	8	13,87	2,65	9,75	8,19	4,10
Usuarios de internet (miles)	14.036,5	6.153,6	4.300	150.0	3.220	2.312,7	300,0
Usuarios de internet por cada 100 personas	13,38	16,10	27,9	1,32	11,61	8,84	9,46
Teléfonos fijos cada 100 personas	17,22	22,76	21,53	6,78	7,49	12,78	11,85
Teléfonos celulares cada 100 personas	36,64	34,76	62,08	0,67	14,85	32,17	26,98

Se observa que todos corresponden a países de América Latina, que hoy día tienen inclinación a la computarización miniaturizada, pues la estadística se concentra en el uso de teléfonos celulares y en segundo término en el uso de Internet.

CONCLUSIÓNES

El creciente y significativo avance que ha generado el desarrollo, difusión y uso generalizado de la informática y su reciente impacto en la sociedad mexicana, despierta con la explosiva incorporación del Internet, que de modo inevitable está presente en todos los ámbitos del quehacer humano, revolucionando los patrones de comportamiento y por ende las relaciones sociales.

La protección jurídica de los programas de computación y las bases de datos es un hecho en el ordenamiento jurídico mexicano, es por eso que nos encontramos con artículos en el código penal sobre el acceso ilícito a sistemas y equipos de informática, en el código civil, en el código mercantil y en mas ya que nos estamos refiriendo a un tema muy amplio con una posible evolución día a día.

En la actualidad en cuanto al Derecho Informático se refiere los delitos mas populares son los penales es por eso que al hacer mis comparaciones con los demás países, noté que Venezuela tienen a bien una ley exclusiva para regular delitos informáticos.

Es importante crear un código en México ya que en mi análisis me doy cuenta que hay muy pocos artículos que regulan los delitos informáticos en el código penal y me di la tarea de buscar noticias de delitos que hayan ocurrido en nuestro país, para darnos cuenta en que articulo se encuentra relacionado y cuales hacen falta en nuestra legislación tomando en cuenta los acontecimientos en el mundo que cada vez surgen con el avance de la tecnología.

Al saber que hay una cantidad enorme de delitos y actos que irán evolucionando a la par de la tecnología, nos damos cuenta que existen leyes que ya lo regulan en México pero también existe la necesidad de una ley que se encuentre enfocada únicamente en los delitos informáticos como existe ya en otros

países del mundo para un mejor entendimiento, es por eso que en esta tesis doy algunos motivos por los cuales se necesita dicha ley.

El Derecho Informático no puede, aunque deseara, formar parte de los departamentos jurídicos o de normatividad tradicionales, debido a las destacadas diferencias particularidades de la materia como:

El Hecho de que su campo de investigación es internacional en la búsqueda de consensos aplicables en interacción con otros países y respetuoso, también, de leyes nacionales.

La mejor herramienta es el estudio de Derecho Comparado. sus fuentes de información generalmente no pueden ser los libros, porque su investigación se sitúa antes de que estos sean publicados. La mayoría de las veces serán sus fuentes de información las revistas especializadas o los documentos y memorias de los congresos en materia de Derecho Informático.

La coordinación de soluciones en Derecho e Informática, y orientadas hacía el bien común, indudablemente beneficiaría al sector productivo, incluyendo un ensanchamiento en las tareas de investigación en la interdisciplina de ambas materias y también en la promoción industrial doméstica basada sobre principios descubiertos en esa investigación y con óptima posibilidad exitosa.

El pensamiento jurídico es por esencia un sistema evidencial por lo que tendrá que concluirse: que el problema jurídico a resolver, y con el objeto de atender esta rama del Derecho, habrá de basarse en la ordenación de un conjunto de evidencias en lo informático, para que el pensar jurídico fundamentado de esas evidencias informáticas de repercusión legal conduzcan al Derecho Informático en una legislación específica que lo haga vigente.

La creación de un centro, con la debida personalidad jurídico-administrativa en Derecho Informático, sería deseable para enfocar y abarcar todas las articulaciones interrelacionadas de la informática y el Derecho en su contexto de problemática nacional, para hacer posible el control de las actividades informáticas desde una legislación que brinde seguridad jurídica.

BIBLIOGRAFÍA

- Azurmendi, Ana. Derecho a la información, Guía jurídica para profesionales de la comunicación. Pamplona: Ediciones de la Universidad de Navarra, 2002 p. 30-32.

- Cuervo Álvarez, José. Delitos Informáticos: Protección pena de la intimidad. España: Ávila, 1998. p. 3

- Floresgómez González, Fernando. Introducción al estudio del derecho y derecho civil. México: Porrúa,2004 p.2

- García Máynez, Eduardo. Introducción al Estudio Del Derecho. México: Porrúa, 2004. P.36

- Gómez Perals, Miguel. "Los Delitos Informáticos en el Derecho Español" Revista iberoamericana del Derecho informático, volumen ISSN 1136-288X. Ejemplar cuarto (1994): 481-496.

- Herrera Bravo, Rodolfo. "Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena" Ponencia presentada en el X Congreso Latinoamericano y II Iberoamericano de Derecho Penal y Criminología de la Universidad de Chile (1998)

- Jirón Ramírez, Maria Eliana. Conceptos de estudios de usuarios. Chile: Escuela de Bibliotecología, 2001 p.2

- Ostalé García, Julio Notas para el concepto de información semántica. España: Universidad de Salamanca, 2006 p.3

- Porrúa, artículos 211 bis 1 al 211 bis 7, Código Penal Federal de México, páginas 70- 71.

- Romeo Casabona, Carlos María. Poder Informático y Seguridad Jurídica. Madrid, España: Fundesco.

- Ruyer Raymond. La cibernética y el origen de la información. México: Colección popular, 1984 p.11

- Téllez Valdez, Julio. Derecho informático: Informática objeto del derecho. México: Mc. Graw, 1997 p.86

- Villanueva, Ernesto. Derecho mexicano de la información. México: Oxford, 2000, p. 298

- Moto Salazar, Efraín, Miguel José Moto. Elementos del derecho. México: Porrúa, 1996 p.7

- Pérez Luño, Antonio Enrique, Ramón Luis Soriano Díaz, Carmelo José Gómez Torres. Diccionario jurídico. Filosofía y Teoría del Derecho e Informática Jurídica. Granada: Comares, 2004.

HEMEROGRÁFICAS

- "Alertan crecen fraudes". Editorial. "Tribuna del Yaqui". 29 de Septiembre del 2007.

- Causan graves perdidas los fraudes cibernéticos". Editorial. "Tribuna del Yaqui". 14 de octubre del 2007.

- Gabriela Cabrera. "Ignoran a victimas del fraude". Editorial. "Tribuna del Yaqui" 18 de octubre del 2007

- Gabriela Cabrera "Desprotegen robo de banca en linea". Editorial. "Tribuna del Yaqui". 18 de Octubre del 2007.

- Lilia Chacón. "sufren firmas robo en la red". Editorial: "Tribuna del Yaqui" 29 de septiembre del 2004.

FUENTES ELECTRONICAS

- Analia Lancillota. " Definición y significado de informática" Revista digital Master Magazín. On line. (http://www.mastermagazine.info/termino/5368.php).

- aprovechan delincuentes ingenuidad de usuarios para fraudes bancarios"yahoo noticias. 19 de septiembre de 2007. On line. (http://mx.news.yahoo.com/s/19092007/7/negocios-aprovechan-delincuentes-ingenuidad-usuarios-fraudes-bancarios.html) [consultado el 22 de septiembre 2007].

- Arturo Trueba. "¿usted como se protege?".Iron port Mundo Ejecutivo.8 de septiembre de 2006. On

line.(http://www.ironport.com/ar/company/mundo_ejecutivo_08-09-06.html) [visitada el 22 de septiembre del 2007].

- "Construir la sociedad de la información: Un desafío global para el nuevo milenio" Cumbre Mundial sobre la Sociedad de la Información: Ginebra 2003-Túnez 2005.12 de mayo de 2004. On line. (http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!MSW-S.doc) [consultada el 24 de Octubre de 2007]

- Claudio Libano Manzur. "Los Delitos de Hacking en sus Diversas Manifestaciones" Alfa-redi revista virtual de derecho informático. On line. Abril 2000. (http://www.alfa-redi.org/rdi-articulo.shtml?x=453) [consultada 25 de octubre 2007]

- Código Penal Federal" Cámara de diputados H. Congreso de la Unión. On line. (www.diputados.gob.mx/LeyesBiblio/pdf/2.pdf) [consultado 13 de septiembre del 2007].

- "código federal de procedimientos civiles" Cámara de diputados H. Congreso de la Unión. On line. (www.diputados.gob.mx/LeyesBiblio/pdf/6.pdf) [consultado 13 de septiembre del 2007].

- Correos falsos de Agencia Tributaria solicitan datos bancarios" Delitos informaticos.com. 13 de Agosto del 2007. On line. (http://www.delitosinformaticos.com/08/2007/delitos/fraudes/correos-falsos-de-agencia-tributaria-solicitan-datos-bancarios) [consultada el 30 de octubre del 2007]

- "crece robo de identidad en la red por falta de precaución de usuarios" Seguridad en Internet… es México. 25 de octubre del 2007. (http://www.emexico.gob.mx/wb2/eMex/eMex_10829_not325_crece_robo_de) [consultada 30 de octubre de 2007].

- "crece 80% el robo de información de empresas" El economista. com.mx. 19 de julio de 2007. On line. (http://www.economista.com.mx/articulos/2007-07-19-40849)[consultado 22 de septiembre del 2007].

- "Detenidos seis crackers por fraudes de phising". Delitos informaticos.com. 26 de diciembre del 2006. On line. (http://www.delitosinformaticos.com/12/2006/delitos/fraudes/detenidos-seis-crackers-por-fraudes-de-phising) [consultada el 30 de octubre del 2007]

- "Derecho informático" Enciclopedia libre electrónica wikipedia.

Online. (http://es.wikipedia.org/wiki/Derecho_inform%C3%A1tico) [consulta 7 de septiembre 2007].

- "Definición y significado de derecho informático" Master Magazín Revista digital líder en informática. Internet: (http://www.mastermagazine.info/termino/4584.php) [consultada 22 de octubre de 2007]

- "Detenido ex-empleado de ViewSonic por piratería informática" Delitos informaticos.com. 11 de Febrero del 2003. On line.

- (http://delitosinformaticos.com/noticias/104498100879682.shtml) [consultada el 30 de octubre del 2007]

- Eduardo Arcos "Ingeniería social para obtener más crédito en el móvil" Altio40 dosis diaria para adictos a la información. On line. 9 de Junio de 2006. (http://alt1040.com/archivo/2006/06/09/ingenieria-social-para-obtener-mas-credito-en-el-movil/) [consultada el 22 de septiembre del 2007].

- Eduardo Martínez Cantero. "se dispara en México numero de fraudes banqueros por Internet" La Jornada, economía. 3 de diciembre del 2006. On line. (http://www.jornada.unam.mx/2006/12/03/index.php?section=economia&article=027n1eco) [visitado el 22 de septiembre del 2007].

- "El Sistema de Banca en Línea, Una Caja Negra Insegura" Robos Bancarios.com, Ausbanc México. 17 de marzo de 2007. On line. (http://www.robosbancarios.com/2007/03/el_sistema_de_banca_en_linea_u.html#more) [consultado el 22 de septiembre de 2007]

- Evangelina Flores "La evolución del derecho a la información en México" Realidad Jurídica. On line. Internet: (http://realidadjuridica.uabc.mx/realidad/contenido-informacion.htm) [Consultado 20 de Octubre del 2007].

- Guillermo López Portillo. "señales robadas". Esmas.com. 6 de febrero 2003. On line. (http://www.esmas.com/NASApp/portal/Noticieros/nt_noticieros_rep.jsp?id=276028) [consultada el 22 de septiembre del 2007].

- Héctor Ramón Peñaranda Quintero. "La informática jurídica: mecanismo de gestión de la información jurídica" 1er Congreso ONLINE del Observatorio para la CiberSociedad. On line. http://www.cibersociedad.net/congreso/comms/c13penaranda2.htm) [21 de Octubre del 2007].

- Jorge Machado. “Hackers, crackers, piratas, phreakers, spoofers, delincuentes informáticos”. Perantivirus. On line. (http://www.perantivirus.com/sosvirus/general/hackers.htm) [consultada el 29 de octubre del 2007].

- Más del 60% de casos de peritaje informático se deben a sabotaje en las empresas, según Recovery Labs” Delitos informaticos.com. 18 de Abril del 2007. On line. (http://www.delitosinformaticos.com/04/2007/seguridad-informatica/mas-del-60-de-casos-de-peritaje-informatico-se-deben-a-sabotaje-en-las-empresas-segun-recovery-labs) [consultada el 30 de octubre del 2007]

- Marcelo Huerta Miranda. “Figuras delictivo - informáticos tipificadas en Chile” Alfa-redi revista virtual de derecho informático. 20 de Marzo del 2002. On line. (http://www.alfa-redi.org/rdi-articulo.shtml?x=433)

- “Primera fase, Ginebra: La cumbre” Cumbre mundial sobre la sociedad de la información: Ginebra 2003-Túnez 2005. 17 de Enero del 2006. On line. (http://www.itu.int/wsis/basic/about-es.html) [consulta 15 de septiembre de 2007]

- “Que es y que no es un hacker” Delincuentes digitales. On line. (http://www.geocities.com/delincuentes_digitales/anteced.htm) [consultada el 29 de octubre del 2007]

- Rafael Guadarrama. “Hacker, un oficio por pasión a la informática” Once Noticias. On line. 6 de junio del 2006. (http://oncetvipn.net/noticias/index.php?modulo=despliegue&dt_fecha=2006-06-06&numnota=43) [consultada el22 de septiembre del 2007].

- Siura Arregoitia López, “Rasgos afines de los llamados delitos informáticos” Buscalegis. On line. (http://www.buscalegis.ufsc.br/arquivos/rasgos_afines.htm) [consultada el día 22 de octubre del 2007].

- Términos y condiciones de uso de mercado libre”.Mercado libre México. On line. (http://www.mercadolibre.com.mx/seguro_terminos.html) [consultada el 30 de octubre del 2007]

- Víctor Rodríguez Hernández. “La informática jurídica y su papel en el Derecho Mexicano” Alfa-Redi Revista de Derecho Informático electrónica. On line. 7 de

Febrero del 1999, (http://docente.ucol.mx/daniel_or/public_html/Marcot.doc) [consultada 04 de octubre de 2007]. ISSN 1681-5726 No.

- Yarina Amoroso Fernández. “Sociedad de la información: Contribución de la Informática Jurídica” Alfa-redi revista virtual de derecho informático. Julio del 2002. On line. (http://www.alfa-redi.org/rdi-articulo.shtml?x=1483) Cuba No. 048

- “13 amenazas ciberespaciales” CNN expansion.com. 20 de septiembre 2007. On line. (http://mx.news.yahoo.com/s/20092007/65/n-business-13-amenazas-ciberespaciales.html)
- [consultada el 22 de septiembre 2007].

ANEXOS

A continuación algunas noticias de delitos informáticos en México:

APROVECHAN DELINCUENTES INGENUIDAD DE USUARIOS PARA FRAUDES BANCARIOS[54]

Miércoles 19 de septiembre, 04:49 PM

Aparecen en México de 200 a 300 sitios falsos de Internet al mes México, 19 Sep (Notimex).- La parte más débil de la cadena de seguridad en el sistema financiero es el usuario, por lo que es necesario aumentar su cultura en la materia, aseguraron expertos de Banamex.

El director de Prevención de Fraudes de esa institución, Liberto Ferrer, sostuvo que la "inocencia" o desconocimiento de los usuarios de la banca es lo que aprovechan los delincuentes para cualquier tipo de fraude, desde el asalto simple hasta el robo de identidad.

Al participar en el Tercer Congreso Internacional de Seguridad, alertó que los patrones de fraudes cada vez son más sofisticados, pero van dirigidos en especial a las personas físicas o a las empresas, por lo que los usuarios de la banca deben tomar ciertas precauciones al momento de realizar sus operaciones.

Hoy la parte más débil es el cliente, la banca ha invertido millones de dólares para blindar sus accesos y su información, la banca está protegida contra la delincuencia, aseguró

---

54 "aprovechan delincuentes ingenuidad de usuarios para fraudes bancarios"*yahoo noticias*. 19 de septiembre de 2007. On line. (http://mx.news.yahoo.com/s/19092007/7/negocios-aprovechan-delincuentes-ingenuidad-usuarios-fraudes-bancarios.html) [consultado el 22 de septiembre 2007].

Ferrer resaltó que además existe en México un comité interbancario, un sistema de alertas nacionales y la afiliación de comercios más seguros, entre otras medidas que ha puesto en marcha la banca para prevenir los fraudes.

Al respecto, el especialista de Banamex, Hugo Montes Campos, subrayó que la delincuencia ha evolucionado del simple asalto, a la falsificación, a la estafa y en los últimos años al uso de la tecnología para cometer delitos.

De esta manera, cada mes aparecen en el mundo entre 30 y 40 mil sitios falsos y en el caso de México cada mes aparecen en internet entre 200 y 300 páginas apócrifas.

Ante este panorama, el especialista de Banamex pidió no dar respuesta a los correos que provengan de estos sitios, pues ninguna institución financiera pide datos personales a sus cuentahabientes.

Recomendó también no abrir ligas o archivos adjuntos, no utilizar computadoras de sitios públicos como los café internet, hoteles o aeropuertos y no escribir las contraseñas.

Subrayó que 99.9 por ciento de los ataques de la delincuencia van dirigidos a los usuarios de la banca, pues el simple hecho de tirar a la basura algún estado de cuenta bancario puede ser utilizado para robar la identidad del cuentahabiente.

Subrayó que en México el nivel de fraudes se ha incrementado y los delincuentes utilizan patrones de conducta parecidos al de los clientes para evitar operaciones sospechosas.

Finalmente, adelantó que entre las medidas que implementará próximamente la banca para disminuir el nivel de fraudes está la validación positiva que consiste en

que al momento de realizar alguna transacción electrónica en algún comercio, se le haga al cliente una pregunta aleatoria para autentificar su identidad

LA JORNADA[55]

Se dispara en México número de fraudes bancarios por Internet. (De enero a octubre la Condusef recibió 640 quejas de víctimas de estafa por ese medio)

Plantea directivo de Banorte doble autentificación para usuarios que manejan grandes cantidades.

Reconocen autoridades que los delincuentes cibernéticos son cada vez más sofisticados.

Por: EDUARDO MARTINEZ CANTERO.

El aumento de los fraudes bancarios por Internet ha impedido que este sector del sistema financiero logre un desarrollo óptimo, toda vez que los usuarios prefieren asistir a las sucursales para realizar de la forma tradicional sus transacciones, por lo que las instituciones bancarias deben invertir en los mecanismos de seguridad que garanticen el resguardo de sus recursos.

De acuerdo con cifras de la Comisión Nacional para la Protección de los Usuarios de Servicios Financieros (Condusef), de enero a octubre de este año esta dependencia recibió 640 quejas de víctimas de fraude electrónico, las cuales reportaron pérdidas por 215 millones de pesos, una cifra superior a la registrada el año pasado, donde el organismo atendió sólo 47 casos, por una cifra no mayor a los 10 millones de pesos.

Héctor Abrego Pérez, director de Canales Electrónicos del Grupo Financiero Banorte, dijo que actualmente un número confidencial o password no es suficiente para garantizar que las transacciones que se realizan por Internet tengan un buen fin, por lo que los bancos están obligados a invertir en herramientas que eviten que los defraudadores sigan cometiendo ilícitos en la red.

---

55 Eduardo Martínez Cantero. "se dispara en México numero de fraudes banqueros por Internet" *La Jornada, economía*. 3 de diciembre del 2006. On line.
(http://www.jornada.unam.mx/2006/12/03/index.php?section=economia&article=027n1eco) [visitado el 22 de septiembre del 2007].

Durante su participación en el foro organizado por la Red Mundial contra el Fraude en Línea, organizado por RSA, filial de la empresa de tecnología EMC Corporation, el directivo de Banorte explicó que para los usuarios identificados como de alto riesgo entre los que se encuentran aquellas personas físicas o empresas que manejan grandes cantidades de dinero, siempre debe existir una doble autentificación que permita al banco estar seguro de que quien está realizando la operación es en realidad el titular de la cuenta. "En este tipo de mecanismo, hemos invertido 15 millones de dólares en los últimos cinco años", apuntó Abrego. Por su parte, Rafael Avante Juárez, director general de Servicios Legales de la Condusef, agregó que si bien en México el problema de los fraudes en línea no es "todavía" severo, sí se deben desarrollar dispositivos de seguridad que den confianza a los usuarios. Detalló que hasta la fecha los montos robados en el país en los que están involucrados clientes bancarios no son "significativos", pero es un problema que crece rápidamente debido a que los delincuentes son cada vez más sofisticados, incluso han rebasado a las autoridades, que no cuentan con la organización que las mafias electrónicas tienen para operar en todo el mundo. Sin embargo, con el apoyo de la Policía Cibernética y para delitos contra menores, de la Policía Federal Preventiva (PFP), se detectaron en lo que va de 2006, 2 mil diferentes tipos de procesos que sirven para robar las contraseñas de los usuarios de servicios de banca en línea entre éstos los denominados phishing, troyanos, virus, espías y spam, que llegan por correo electrónico, además de que se desactivaron 470 sitios por medio de los cuales se defraudaba a la gente. Por ello, la recomendación es que cuando se detecte un e-mail sospechoso sea reenviado a: alertasphishing@ condusef.gob.mx. Avante mencionó que en el país se requieren campañas de información que le digan a las personas cómo protegerse de este tipo de ilícitos, acompañadas de herramientas legales que permitan desactivar de inmediato un sitio ilegal y que involucre a los bancos cuando de respaldar al usuario afectado se trate, pues las instituciones bancarias no se hacen responsables de este tipo de casos. Christopher Youn, representante de RSA, señaló que este tipo de fraudes son sólo un eslabón más de una gran cadena del crimen organizado, donde los recursos que se obtienen por el robo a clientes bancarios sirven para financiar

delitos mayores. Explicó que 50 por ciento de los delitos cibernéticos tiene su origen en Estados Unidos, lo cual no significa que los ciberdelincuentes vivan en ese país, pues las bandas están tan bien organizadas y cuentan con la tecnología para operar desde cualquier otra parte del mundo. Por la red no sólo se pueden cometer fraudes, según la PFP los delitos más comunes son las amenazas por correo electrónico, el robo de identidad (para comprar artículos con el nombre de otra persona o para culpar a otros cuando se comete un delito), difamaciones, ciberterrorismo y lo que se conoce como ingeniería social (personas que con el fin de obtener información se hacen pasar por otras u obtienen sus claves personales para cometer fraudes).

Hacker, un oficio por pasión a la informática [56]

Existe un mundo intangible llamado internet. Ahí todo son códigos, passwords o claves de usuario. Es por ello que para algunos, él pudiera ser Braulio, pero de lunes a jueves, desde hace cinco años, cada vez que coloca las manos sobre el teclado de su computadora, cambia de identidad más que por ocupación, por pasión a la informática. Braulio es un joven hacker.

"Red Point, 17 años, y por el momento me dedico a verificar vulnerabilidades en sitios web importantes, reportándolos para así tener una esperanza de que ofrezcan trabajo o que den algo a cambio, pero antes me dedicaba al deface de webs", comentó Braulio. Sus conocimientos los desarrolló a los 12 años, cuando aprendió a programar en internet. Con la práctica, pudo ingresar de forma clandestina a servidores y páginas entre ellas la de la SEP y Colegioweb, donde modificó sus calificaciones. Sin embargo, esto le trajo desagradables consecuencias.

56 Rafael Guadarrama. "Hacker, un oficio por pasión a la informática" *Once Noticias*. On line. 6 de junio del 2006. (http://oncetvipn.net/noticias/index.php?modulo=despliegue&dt_fecha=2006-06-06&numnota=43) [consultada el22 de septiembre del 2007].

“Tomé el control, cambié calificaciones y me cacharon porque una exnovia me delató”, recordó Braulio. Motivado por el rencor, encontró el modo acceder nuevamente a las 95 páginas de Colegioweb, desactivarlas, y dejar un mensaje. “-Les dejé la firma, con un mensaje a la directora de la escuela.
¿-Y qué decía el mensaje? Decía: al profesor de computación le puse que se dejara de propasar con las niñas y que enseñara computación, y a la maestra le puse: saludos a la tonta directora”.

Braulio afirma haber intervenido unas 32 mil páginas, cinco de ellas de gobierno, lo cual le ha demostrado que con empeño, no hay puertas que puedan estar cerradas para él. Muchos jóvenes como Braulio ven en el trabajo del hacker un juego, muchas veces sin la conciencia de que se trata de una actividad ilegal.

“Está cometiendo un delito. El adolescente que está entrando en esas lides debe saber que está entrando en un terreno fangoso, un terreno que le va a traer problemas ya que está causando problemas a un tercero que normalmente es un tercero que no conoce, que nunca le hizo daño y que no tiene por qué hacerlo”, dijo Roberto Massa, director comercial del Área de Consumo de Symantec.

La curiosidad de los jóvenes hacker los puede llevar a descubrir vulnerabilidades en línea de sistemas bancarios, y así robar números de cuenta de clientes y en ocasiones, su contenido.

“El tener control sobre una sesión abierta implica que si estaba uno a la mitad de consultar banca electrónica puede el atacante en efecto, hacerse un depósito, un retiro”, manifestó Víctor Chapela, director general de Smart.

para algunos expertos, esta situación es la que marca el futuro del hacker. Generalmente los jóvenes poco habilidosos son quienes sucumben ante las mieles del fraude, las cuales en rara ocasión eluden las sanciones de la policía.

Si bien la motivación de los jóvenes por el hackeo se enmarca entre la aventura de la ilegalidad, también influye en gran medida el gusto por aprender nuevas cosas.

“El hecho de que puedan burlar las normas, puedan brincarse las trancas, romper las reglas, introducirse en otras cosas, son retos muy interesantes, son retos mentales”, opinó Carlos Lang Merino, vicepresidente de seguridad de Amipci

Y el problema que enfrentan los jóvenes en este sentido, es que las escuelas, particularmente en las materias de computación, muy pocas veces brindan conocimientos que desafían sus mentes.

“Eso se está dando ya desde primaria, hemos visto ya casos de alumno de primaria que ya se burlan a los maestros, y probablemente sepan mucho más que los maestros, entonces ya hay niños de entre los 6, 8 años que están empezando a operar estas cosas”, informó Carlos Lang Merino, vicepresidente de Seguridad de AMIPCI.

Por ello, la importancia de actualizar la enseñanza, ya que en general los hackers con el paso de los años terminan siendo los responsables de diseñar los sistemas informáticos de seguridad de las grandes empresas.

“Te vas a encontrar a los niños que ya crecieron y que actualmente son consultores de seguridad, que trabajan con bancos, que trabajan con policías, con agencias de investigación y están encausando todas esas habilidades. Un hacker no se va a hacer millonario, pero un consultor de seguridad puede llegar a ser un buen empresario, puede llegar a tener un trabajo bastante bien remunerado”, concluyó Lang Merino.

Y justo eso busca Braulio. Tras recibir una llamada preventiva de la PGR, ahora intenta aprovechar sus conocimientos para mejorar la seguridad de páginas de internet.

Ingeniería social para obtener más crédito en el móvil[57]

Recientemente he notado una pequeña ola de comentarios con cierta similitud en posts medianamente populares de este blog, por ejemplo:

Juan Carlos Díaz | powerboy20@hotmail.com
SALDO GRATIS PARA USUARIOS TELCEL Solo manda un msj de texto con el numero: 811026594313 (lleva un espacio antes del 13) al # 7373 y tu saldo se duplicara solo espera la confirmación con un mensaje de texto y listo
¡¡¡¡espero que lo disfrutes!!!!!!!!!!

La idea es hacerle creer a las personas que pasan por ahí (o que buscan "saldo gratis telcel" por ejemplo, que al escribir esa serie de números que más parece una clave secreta duplicarán su saldo disponible, ingeniería social simple, pero algo me dice que muy efectiva.

El hecho es que esos números transfieren saldo de la persona que lo escribe al número celular: 8110265943, por la cantidad de 13 pesos. El enviar el mensaje al número 7373, la transferencia de saldo se realiza para usuarios de prepago de Telcel.

Un tanto ingenioso, aunque el tal Juan Carlos se ganará algunos insultos por teléfono con las personas que se den cuenta del truco; a menos, claro, que nadie conteste ese teléfono y sólo se use como un "receptor". No dudo que veamos este tipo de cosas en un futuro cercano con números de teléfono de personas dentro de cárceles que quieren obtener crédito para realizar esos fraudes o secuestros express

57 Eduardo Arcos "Ingeniería social para obtener más crédito en el móvil" *Altio40 dosis diaria para adictos a la información.* On line. 9 de Junio de 2006. (http://alt1040.com/archivo/2006/06/09/ingenieria-social-para-obtener-mas-credito-en-el-movil/) [consultada el 22 de septiembre del 2007].

13 amenazas ciberespaciales[58]

Los ciberdelincuentes se están profesionalizando y cada vez más desarrollan, distribuyen y emplean códigos y servicios maliciosos para atacar a quienes navegan por la red y obtener ganancias económicas, advirtió el líder mundial en software de infraestructura, Symantec, en su Informe sobre Amenazas a la Seguridad en Internet.

Las amenazas que se propagan a través de Internet y la actividad maliciosa que estamos analizando en estos momentos, indican que los hackers están llevando esta tendencia al siguiente nivel, convirtiendo en su profesión los delitos en la Red, empleando para ello prácticas de tipo empresarial para lograr con éxito sus objetivos, afirmó el vicepresidente de Symantec Security Response, Arthur Wong.

La compañía detectó entre el primero de enero y el 30 de junio de este año un alza en el número de delincuentes que están utilizando paquetes de herramientas para atacar a los cibernautas.Conoce las principales tendencias de ataque detectadas por Symantec:

Estados Unidos fue el país con más ataques en donde se negó el servicio (DoS) al registrar el 61% del problema a escala mundial en la primera mitad de 2007. Estados Unidos fue el principal país de origen de ataques, con 25% del total mundial. El 30% de la actividad maliciosa se concentró en Estados Unidos. Israel registró la mayor actividad maliciosa en la red por usuario de Internet, seguido de Canadá y Estados Unidos. 4% de toda la actividad maliciosa detectada en la red se originó en direcciones registradas de empresas en la lista Fortune 100. El sector

58 "13 amenazas ciberespaciales" *CNN expansion.com*. 20 de septiembre 2007. On line. (http://mx.news.yahoo.com/s/20092007/65/n-business-13-amenazas-ciberespaciales.html) [consultada el 22 de septiembre 2007].

educación tuvo el 30% de las fallas en seguridad que pueden llevar al robo de identidad. Las tarjetas de crédito fueron los artículos más anunciados en servidores del mercado negro (22%), seguidas por las cuentas bancarias (21%). El 85% de los números de tarjetas de crédito que se vendían en el mercado negro del Internet fueron emitidas por bancos estadounidenses y únicamente un uno por ciento provino de bancos en México.

Durante el primer semestre de 2007, se conocieron 237 vulnerabilidades que afectaban plug-ins del navegador, un importante aumento frente a las 74 registradas en la segunda mitad de 2006 y 34 en el primer semestre de 2006. Los códigos maliciosos que intentaron robar información de cuentas de juegos en la red representaron 5% de las principales 50 muestras de códigos maliciosos con capacidad para producir una infección potencial. Los juegos en la Red se están convirtiendo en una de las actividades más populares y, a menudo, ofrecen artículos que pueden ser adquiriros mediante dinero, lo que proporciona una oportunidad potencial para que los atacantes obtengan beneficios económicos. El spam representó 61% de todo el tráfico de correo electrónico monitorizado, lo que supone un ligero aumento frente a lo registrado el último semestre de 2006, cuando 59% de los correos electrónicos fue clasificado como spam. La pérdida o robo de equipos o de otro medio para almacenamiento de datos representó 46% de todas las fugas de datos que pueden generar suplantaciones de identidad. Symantecs IT Risk Management Report mostró que 58% de las empresas esperan una importante pérdida de datos, al menos una vez cada cinco años. El 95% de las víctimas de los atacantes cibernéticos son usuarios en casa.

¿Usted cómo se protege?[59]

El spam, los virus y códigos maliciosos amenzan a la Red. En México no hay registros oficiales sobte daños generados por ataques informáticos, pero existen 557 casos documentados de fraudes electrónicos, 70% de ellos por cargos

59 Arturo Trueba. "¿usted como se protege?".*Iron port Mundo Ejecutivo*.8 de septiembre de 2006. On line. (http://www.ironport.com/ar/company/mundo_ejecutivo_08-09-06.html) [visitada el 22 de septiembre del 2007].

indebidos en tarjetas de crédito en transacciones realizadas por Internet, con pérdidas aproximadas por 183 millones de dólares.
Si piensa que los gusanos son unos lindos animalitos que viven entre las flores, que Troyanos es el título de una película de acción, que para combatir a los virus sólo requiere medicamentos y reposo o que el phishing tiene que ver con la pesca deportiva, déjenos decirle que está equivocado y que su negocio corre peligro de ser víctima de un ataque electrónico que puede hacerle perder un activo más que importante: la información.

En el mundo virtual aparecen entre 75 y 100 vulnerabilidades malignas cada semana y apenas uno de cada tres usuarios de la Red cuenta con antivirus o firewall en su computadora. Hoy tampoco se salvan de ataques los teléfonos celulares con tecnología bluetooth, GSM o de tercera generación, pues ya existen programas que instalan archivos malignos para extraer información de sus memorias.

De acuerdo con cifras citadas por Gonzalo de Velasco, director general de McAffe México, el valor del mercado de seguridad informática en nuestro país en 2006 es de entre 56 y 75 millones de dólares, debido al creciente peligro y la falta de procesos de control, pues, según datos de la consultora Gartner, 70% de los empleados aún abre archivos recibidos vía e-mail de destinatarios desconocidos, a pesar de las advertencias que se hacen y el enorme riesgo que representa.

En México operan al menos diez asociaciones de hackeo, las cuales provocaron el último año ataques a páginas electrónicas, cuentas bancarias, claves, contraseñas e información confidencial de diversas organizaciones, como la Comisión Nacional Bancaria y de Valores, la Cruz Roja Mexicana, el Tec de Monterrey, el Senado de la República, el INEGI, la Secretaría de Salud, TV Azteca o el gobierno de Yucatán, según documentos de Informatics Institute.

Aunque en México no se cuenta con registros oficiales sobre los daños que generan los ataques informáticos, existen 557 casos documentados de fraudes electrónicos, 70% de los cuales se refiere a cargos indebidos a tarjetas de crédito en transacciones realizadas por medio de Internet, con pérdidas aproximadas por 183 millones de dólares.

Señales robadas[60]

Hoteles y condominios tienen sistemas ilegales de televisión.

El robo de señales de televisión es una cadena de ilegalidad, tanto en condominios residenciales, Como en fraccionamientos de lujo, En hoteles, En tianguis.

En el centro del país, En la frontera norte... Una suma de delitos que atacan la televisión de paga vía satélite:

Robo de señal

Violación a las leyes de derecho de autor

Desciframiento ilegal de señales satelitales.
"Que se den cuenta que es un delito federal, que puede ir hasta cinco años de prisión, no es cuestión de estrato social, este problema lo vivimos en campos de golf, en colonias de muy alto nivel económico, en hoteles", afirmó Jorge Cuevas, presidente de la Cámara de la Industria de Televisión por Cable.

En un lujoso hotel de la ciudad de Guanajuato se encontró un sistema privado de televisión con 9 equipos de la compañía Sky.

60 Guillermo López Portillo. "señales robadas". *Esmas.com*. 6 de febrero 2003. On line. (http://www.esmas.com/NASApp/portal/Noticieros/nt_noticieros_rep.jsp?id=276028) [consultada el 22 de septiembre del 2007].

Las señales se concentraban en una central que distribuía la programación a las habitaciones.

“La señal se estaba subiendo a las habitaciones, sin el contrato correspondiente para ello, los equipos no están registrados, no se tiene una contratación para un uso hotelero”, informó Yamil Melo, Gerente Regional Sky-Guanajuato.

En la azotea se localizaron las antenas de Sky. Varias con el logotipo borrado.

Abogados de la compañía Sky determinaron que los equipos fueron contratadas para servicio residencial en Monterrey y aparecieron en Guanajuato.

El gerente del hotel dice que la responsabilidad es de una empresa de Monterrey, Nuevo León:

“Yo no sé si es legal o no es legal, lo que yo sé es que estábamos con una empresa que nos daba el servicio.” El hotel o la empresa responsable podrían ser multados con más de 800 mil pesos por piratería.

“Tiene tanta culpa el que mata la vaca como el que le agarra la pata, el que lo vendió o el que lo está usando”, afirma Pablo Vázquez, Director de Sky.

Aquí donde un metro cuadrado de terreno se cotiza en más de mil dólares o más de 10 mil pesos se lleva la piratería de señales de televisión.

En un fraccionamiento y club de golf cercano a Toluca se instaló una red de televisión privada con programación de varias compañías satelitales.

Usando una cámara oculta, el equipo de Los Reporteros habló con el instalador:

¿Y desde dónde viene el cable?... Casi desde la caseta de vigilancia... ¿Ya vamos a ver todos los canales? 24, 25, 26, más o menos ¿Cómo bajan la señal? Todo es vía satélite.

El servicio de televisión se ofrecía a través de un volante... De una empresa fantasma.

Después de buscar por varias zonas del fraccionamiento, el equipo de investigaciones especiales encontró las antenas escondidas entre la vegetación y protegidas por bardas.

Acudimos a la administración del fraccionamiento y club de golf a pedir una explicación.

Aquí presentamos la respuesta:

Yo no tengo nada que ver en esto, yo nada más le quiero informar que el señor a través de su secretaria me informo que mañana va a estar aquí a las 11... ¿Y ahorita dónde lo podemos localizar?... No... Ya, ya, ya...

El representante del fraccionamiento se comprometió a desmantelar el sistema de televisión irregular, aunque se negó a dar una entrevista.

Ningún particular puede tener una red de televisión sin una autorización expresa de la SCT.

En Bosques de las Lomas, una de las zonas más exclusivas de la Ciudad de México también ocurre el robo de señales.

Usted no va a ordenar lo que se va a hacer, a mi me autorizan a romper chapas, si usted no me deja entrar, voy a romper las chapas... Yo no me estoy oponiendo, sólo quiero llegar a un acuerdo.

En el sótano de una de las Torres de Bosques de Reforma funcionaba el cerebro del sistema de televisión.

En estos lujosos departamentos se veía por ejemplo el canal permanente de Big Brother sin el pago correspondiente por suscriptor a la compañía Sky.

Al parecer estaba incluido en la cuota de mantenimiento, todos los vecinos tiene este tipo de servicio y lo incluyen en una cuota de mantenimiento.

El Ministerio Público de la Federación aseguró equipos decodificadores y antenas.

Héctor Ávila, Fiscal Antipiratería de la PGR señaló que se estaban cometiendo tres delitos, dos en materia de derechos de autor y el denominado robo de fluido, que es un robo equiparado.

En el territorio nacional alrededor de 700 hoteles y condominios tienen instalados sistemas ilegales de televisión privada.

“Y que obviamente genera pérdidas para todos, para nosotros los proveedores de señales, para la gente provee los canales, para los distribuidores que tiene una estructura de instalación, de comercialización y de montaje”, señala Roberto Sierra, director de DirecTV México.

El aumento de impuestos y la piratería han provocado el estancamiento de la industria de televisión de paga y el recorte de empleados.

Omar Robles es ingeniero en comunicaciones electrónicas... Se dedicaba a orientar antenas satelitales... Ahora vende hamburguesas en calles del Municipio de Ecatepec.

Omar ha buscado trabajo en más de 50 lugares, sin conseguirlo:

“No tenemos conciencia lo que puede acarrear robarnos una señal de televisión, puede acarrear desempleo, puede acarrear que muchas familias se queden sin trabajo.

Cada equipo de televisión satelital de paga requiere de una tarjeta inteligente para operar.

Contiene un programa de cómputo que indica que canales abrir para el suscriptor.

En mercados y tianguis como el de La Raza se ofrecen a la venta equipos de recepción de satélite y tarjetas inteligentes violadas o clonadas.

Un equipo de Los Reporteros acudió con cámara oculta al Mercado de La Raza:

“¿Cuál nos consigues? El Sky y el Directv y hay uno nuevo que va a entrar que es el Dish, parecido al Direct... Trae mucho más canales... En 7, 500 ¿Todo abierto? Todo abierto.”

Los vendedores de equipos y tarjetas piratas o robados se escudan en la más absoluta impunidad.

El principal mercado negro de tarjetas inteligentes se ubica en el centro y norte del país.

Se anuncian en periódicos e Internet.

Proporcionan teléfonos, por lo general celulares, aunque nunca direcciones.

Pablo Vázquez, Director de Sky asegura que hay entre 90 y 100 mil familias en Chihuahua que tienen señales piratas, Tijuana es otro caso, Monterrey.

La PGR y el Instituto Mexicano de Propiedad Industrial advirtieron que continuarán los operativos para combatir la piratería de televisión satelital en todas sus formas.

Crece robo de identidad en la red por falta de precaución de usuarios [61]

Recomiendan utilizar sentido común para protegerse de dicho ilícito.
México DF, 25 Octubre 2005 (Notimex). El robo de identidad a través de Internet es cada vez más frecuente en todo el mundo y México no es la excepción, lo cual obedece en parte a que dicho ilícito ha adoptado diversas modalidades y a la falta de precaución por parte de los usuarios de la red.

En entrevista con Notimex, el coordinador de tecnología de Trend Micro, Daniel Ortiz, indicó que si bien Estados Unidos es el país en donde se registra un mayor número de estos ilícitos, en México también se reportan y por ello los bancos ya toman sus precauciones.

"Se debe destacar que aún no se sabe a ciencia cierta si quienes están robando la identidad a través de la red son hackers o personas que se dedican al fraude en todas sus modalidades", comentó.

Consideró que ya no se trata de aficionados que quieren demostrar su capacidad de diseñar programas para cometer fraudes, sino de personas que actúan en forma premeditada para hacer daño, con un fin particular.

---

61 "crece robo de identidad en la red por falta de precaución de usuarios" *Seguridad en Internet… es México*. 25 de octubre del 2007. (http://www.emexico.gob.mx/wb2/eMex/eMex_10829_not325_crece_robo_de) [consultada 30 de octubre de 2007].

Ante la magnitud del problema, refirió, en Estados Unidos se hacen ya campañas de concientización y se da conocer que el robo de identidad implica que cualquier persona puede hacer todo lo que el dueño de la tarjeta de crédito haría.

El ilícito consiste en que una persona use la identidad de otra para cometer fraudes o en el robo de información, lo cual puede ocurrir de muchas formas, por ejemplo mediante la clonación de tarjetas de crédito o la instalación de falsos cajeros automáticos.

"Pero también lo son el phishing (solicitar información con correos falsos) o el pharming (robo de información a través de páginas falsas), así como el spyware y el spam, los cuales se relacionan más con archivos malignos dentro de correos electrónicos", comentó.

A su decir, el fraude en la red se ha extendido debido a que ha adoptado varias modalidades para adquirir la información o identidad de otros, así como a la falta de precaución de los usuarios al usar la red para transacciones financieras.

"Se debe tomar en cuenta además que cuando se comete un robo o un fraude no es sólo a la persona que se dañó directamente, sino también a la institución como bancos o tiendas en Internet, las cuales sufren pérdidas monetarias y de prestigio", aseguró.

Daniel Ortiz sugirió reportar de inmediato cualquier anomalía, incluso si se trata de un sitio ubicado o registrado en el extranjero, pues a pesar de parecer complicado cualquier persona puede protegerse de padecer un ataque de este tipo, afirmó.

Se trata, apuntó, de tener sentido común y así como una persona se protege físicamente de no sufrir un robo, también lo puede hacer virtualmente en la red; por ejemplo, dijo, no se da a cualquiera el número y clave de tarjeta de crédito, y lo mismo debe evitarse en Internet.

"Se puede verificar si las páginas de los bancos son reales o no dando click a las ligas que aparecen, si estas no llevan a ningún lado pueden no ser reales, además se debe contar con antivirus y firewall en sus máquinas, así como verificar si su proveedor de servicio le ofrece protección antispam y antiphishing", dijo.

Finalmente, el directivo comentó que en la página en Internet de Trend Micro los interesados pueden escanear sus computadoras en forma gratuita para determinar si hay algún programa espía o virus instalado en sus equipos.

Crece 80% el robo de información en empresas[62]

En México, cada año aumenta 80% el número de empresas que sufren de robo de información y contaminación de sus equipos de cómputo, a través de virus, gusanos, malware y spam, informó la empresa Fortinet.
Redacción / El Economista.com.mx

En México, cada año aumenta 80% el número de empresas que sufren de robo de información y contaminación de sus equipos de cómputo, a través de virus, gusanos, malware y spam, informó la empresa Fortinet.

El ingeniero de Aplicación para Latinoamérica de Fortinet, David Ramírez, dijo que este tipo de ataques afectan en mayor índice a Pequeñas y Medianas Empresas (Pymes), las cuales por lo regular carecen de presupuesto y personal para responder de forma eficaz a los incidentes.

Entrevistado, luego de ofrecer la conferencia Seguridad Perimetral-Real Time Netwoorks Protection, expuso que las grandes y pequeñas empresas resultan atractivas para los atacantes, aún cuando si invierten en soluciones de seguridad.

62 "crece 80% el robo de información de empresas" *El economista. com.mx. 19 de julio de 2007. On line.* (http://www.economista.com.mx/articulos/2007-07-19-40849)[consultado 22 de septiembre del 2007].

Por ello, indicó la firma desarrolla soluciones de tecnología de seguridad basada en un Gateway (Appliance) de propósito especifico.

Precisó que la solución integra ocho herramientas de seguridad, en un Gateway: “Todo en uno”, con un avanzado desarrollo tecnológico, seguro, poderoso, de alto desempeño, confiable y de administración sencilla e intuitiva, sin ser excesivamente costosa.

La aplicación se encuentra integrada en una sola plataforma y su costo va de 800 a 50 mil dólares, pero desconoció el tiempo que tardan las empresas en recuperar su inversión, abundó.

La empresa de seguridad ofrece diferentes equipos que pueden ser instalados en todos los sectores de la industria, desde los que tienen una red de 20 computadoras, hasta las que cuentan con una red de ocho mil computadoras, agregó.

Asimismo, reconoció que cualquier empresa con acceso a Intenet necesita de equipos de seguridad de red, en la WEB y correo, además de contar con alta disponibilidad, BandwidthShaping y administración de tráfico, para evitar robo de información y contaminación de virus.

NOTICIAS DE PERIODICOS LOCALES

Tribuna del Yaqui 29 de Diciembre 2004.

Los ciberdelincuentes copian archivos totales con reproductores MP3 y memorias USB.

Grece la ciberdelincuencia

Los robos de secretos industriales a las empresas se facilitó con la masificación de memorias móviles (Robo y pérdida de información)

Fuente: Symantec. Dirección: Edmundo Lagunilla / Agencia Reforma

TRIBUNA 29 DE SEPTIEMBRE 2004
ECONOMIA - PAG

Sufren firmas robo en la red

POR LILIA CHACÓN
AGENCIA REFORMA

C.D. DE MÉXICO.- En México, Mástel 80 por ciento de los ataques que enfrentan las empresas en línea es por robo de información a través de memorias móviles o modificaciones en las aplicaciones web, las cuales tienen la capacidad de copiar por completo los discos duros de las PC, advierten empresas de seguridad.

De acuerdo con el reporte del único laboratorio de cómputo forense en México, Mattica, 8.2 de cada 10 ataques contra las empresas para accesar los secretos industriales y propiedad intelectual son generados por los propios empleados de las organizaciones.

Aunque 34 por ciento de estas personas desconocen que fueron utilizados para este fin, explicó el director de investigaciones de la firma, Andrés Velázquez.

Las principales herramientas que se utilizan para ello, son las memorias móviles y las aplicaciones en línea, agregó el gerente para América Latina de Symantec, Rafael García.

En los robos premeditados, los empleados utilizan sus reproductores de MP3, como el iPod, y memorias USB, con una aplicación denominada "slurping", que le permite copiar la totalidad de los archivos de una PC, aunque el equipo esté bloqueado por un password de acceso, explicó García.

Mientras que los robos involuntarios se dan, debido al bajo nivel de preparación informática de los trabajadores, aspecto que los convierte en presa fácil de los ciberdelincuentes.

"Tan sólo con abrir una página de Internet, pueden ejecutar un programa inadecuado, darle acceso no autorizados a la red, desactivar un programa de seguridad y dar acceso a toda la información de la compañía", detalló Velázquez.

Una tercera vía de acceso, son las aplicaciones de autoservicio que dan las empresas a sus clientes, socios y proveedores en sus páginas web, pues a través de ellas los atacantes pueden correr una aplicación para accesar a toda la información de la empresa, si los sistemas no están bien configurados, afirmó García.

Prueba de ello, comentó el directivo de Symantec, fue el crecimiento de más de tres veces en el desarrollo de códigos maliciosos que se dio a nivel mundial, con más de 212 mil nuevas amenazas en los primeros seis meses del año.

Los riesgos van en aumento, con la adopción de las herramientas de colaboración en línea, como parte de la evolución hacia la web 2.0, donde es más complicado para las empresas tener el control de los accesos y de la información, que es generada y controlada por los usuarios en lugar de las organizaciones, agregó García.

Alertan crecen fraudes

STAFF DE REDACCIÓN
TRIBUNA

Hermosillo.- Ante la delegación de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) se han registrado en el presente año, quejas de por lo menos quince usuarios, afectados con "fraudes electrónicos".

Marco Arturo Moreno Ward, delegado de la CONDUSEF, precisó que de este total, once casos están en proceso de una respuesta de parte de las instituciones financieras, mientras que dos pudieron conciliarse y en dos de estos, no se pudo concretar ningún arreglo para los quejosos.

El funcionario federal, señaló que la utilización de la banca a través de Internet se ha incrementado y con esto, la proliferación de correos electrónicos que no provienen de las páginas oficiales de los bancos.

Dijo que ante lo complicado que resulta la comprobación de estos fraudes, la recuperación en la dependencia es de apenas 26 mil pesos, contra una reclamación superior a los 370 mil pesos.

POR DELITOS EN LA RED

Ignoran a víctimas de fraude

De manera normal no hay métodos lo suficientemente sofisticados para descubrir a los ciberdelincuentes

POR GABRIELA CABRERA
AGENCIA REFORMA

C.D. DE MÉXICO.- Miles de personas que son víctimas de fraudes a través de banca en línea están desprotegidas porque aún no hay un delito tipificado en el Código Penal Federal, y por lo tanto, en el resto del País no se le da asistencia especializada ni se usan métodos sofisticados para descubrir al ciberdelincuente.

Según una revisión de los códigos penales de las entidades federales, aunque en el DF, Puebla y Chiapas se reconoce que existe la posibilidad de cometer fraude a través de transferencias electrónicas o mecanismos cibernéticos, no existen garantías suficientes para los afectados.

En las entidades federativas normalmente no existe un tipo penal especial para este delito. Si está tipificado, pero en forma genérica dentro del fraude, que es un delito local", aseguró Jorge Graciela Morafla, socio de la firma Graciela Morafla y Asociados, especialista en el sector financiero.

"El problema principal es que los Ministerios Públicos no tienen la especialización para poder comprender todo el mundo que se realiza en un fraude por medios electrónicos", añadió.

Alfredo Acevedo, socio de la misma firma, señaló que el problema es que los Procuradores de cada Entidad emiten con circulares para establecer criterios en los Ministerios Públicos, y estos varían de un Estado a otro.

Un ejemplo es el DF, donde, aunque está reconocido el fraude vía transferencia electrónica la Circular A/003/99 deja un delito especializado a víctimas de fraudes en línea por robo menores a 758 mil pesos.

Y la fiscalía para delitos financieros sólo los delitos de fraude y abuso de confianza por un monto superior a 15 mil veces el salario mínimo vigente del Distrito Federal", cuando la fracción III del Artículo 28 de la circular.

Miles de personas que son víctimas de fraudes en banca en línea están desprotegidas porque en una entidad del País está tipificado el delito informático, en dos existe la referencia de fraude vía transferencia electrónica y en el resto está considerado como un fraude genérico.

Desprotegen robo de banca en línea

En el DF, el fraude debe ser mayor a 758 mil pesos para ser atendido por la fiscalía especial

POR GABRIELA CABRERA
AGENCIA REFORMA

C.D. DE MÉXICO.- Miles de personas que son víctimas de fraudes en banca en línea están desprotegidas porque aún no hay un delito tipificado en el Código Penal Federal, y por lo tanto, en el resto del País no se le da asistencia especializada ni se usan métodos sofisticados para descubrir al ciberdelincuente.

De acuerdo con una revisión de los códigos penales de las entidades federales, aunque en el DF, Puebla y Chiapas se reconoce que existe la posibilidad de cometer fraude a través de transferencias electrónicas o mecanismos cibernéticos, no existen las garantías suficientes para los afectados.

En las entidades federativas mexicanas normalmente no existe un tipo penal especial para este delito, si está tipificado, pero en forma genérica dentro del fraude que es un delito local", aseguró Jorge Graciela Morafla, socio de la firma Graciela Morafla y Asociados, especialista en el sector financiero.

"El problema principal es que los Ministerios públicos no tienen la especialización para poder comprender todo el mundo que se realiza en un fraude por medios electrónicos", añadió, Alfredo Acevedo, socio de la misma firma, señaló que el problema es que los Procuradores de cada Estado han emitido con circulares para establecer criterios en los Ministerios públicos y estos varían de un estado a otro, explicó Acevedo Rivas.

Cual DF, aunque está reconocido el fraude vía transferencia electrónica la Circular A/003/99 emitida por la Procuraduría General de Justicia local deja un delito especializado a víctimas de fraudes en línea por robo menores a 758 mil pesos.

ECONOMÍA — Ciudad Obregón, Sonora

Causan graves pérdidas los fraudes cibernéticos

A nivel mundial cada año se pierden más de 100 mil millones de dólares por estos delitos

NOTIMEX

C.D. DE MÉXICO.- El investigador Flavio Arturo Sánchez Garfias urgió a reforzar los sistemas de seguridad informática en el País a fin de disminuir los fraudes cibernéticos que a nivel mundial causan pérdidas superiores a 100 mil millones de dólares anuales.

El jefe del Departamento de Programación y Desarrollo de Sistemas de la Escuela Superior de Cómputo (ESCOM) del IPN indicó que los ilícitos de esa naturaleza perjudican tanto a instituciones bancarias, financieras y dependencias, como a la sociedad en general.

Manifestó que de acuerdo con información de organismos financieros internacionales los delitos cibernéticos han afectado a organismos públicos y privados.

Urgen a reforzar los sistemas de seguridad informática en el País.

Dijo que éstos son graves y más si se toma en cuenta que en el País muchas instituciones bancarias no denuncian cuando son víctimas de ellos porque temen que la sociedad no les confíe su dinero.

Explicó que aun cuando se cree que esos ilícitos los cometen los "hackers" (piratas cibernéticos) no es así, ya que a ese tipo de personas que tienen muchos conocimientos sobre computación y manejo de redes les atraen las cuestiones de seguridad informática y tratan de introducirse "por gusto, no por hacerle daño a los sistemas".

De ahí que, añadió, "es un reto para ellos demostrar su habilidad y dominio sobre esa materia".

De acuerdo con Sánchez Garfias en la mayoría de los casos los fraudes cibernéticos son cometidos por "crackers", a quienes les gusta introducirse a los sistemas para dañar a las personas, ya sea alterando sus sistemas, robando o apropiándose de su dinero o de datos confidenciales importantes.

Mencionó que los "crackers" también acceden a grandes empresas transnacionales, a dependencias estratégicas de los gobiernos e incluso llegan a aliarse o son reclutados por bandas de delincuencia organizada.

Ante ello recalcó la necesidad de tomar precauciones para no ser sorprendidos por quienes utilizan la Internet para cometer esos delitos, aunque reconoció que cada vez se detectan más casos en virtud de la alta tecnología disponible.

Con tales ejemplos de noticias podemos imaginarnos el numero de delitos informáticos en México y que al evolucionar la tecnología hace mas necesaria la existencia de medidas de seguridad para los nuevos delitos informáticos, los cuales deberían de estar regulados en una sola ley para su practico entendimiento, ya que de esta forma puede proporcionar al ciudadano un fácil acceso y entendimiento de la ley.