Bogotá, D.C. 4 de Octubre de 2010.

Doctor
CARLOS BERNARDO MEDINA
Director de Postgrado de Derecho
Universidad Libre
Ciudad.

Respetado Doctor Medina:

En cumplimiento de las políticas de la Universidad Libre, presento el Trabajo de Investigación Titulado "**LOS DELITOS INFORMATICOS Y SU APLICACION EN LA LEGISLACION COLOMBIANA"** elaborado por el alumno **JOSE JOAQUIN GONZALEZ CARRILLO.**

La presente investigación es un trabajo desarrollado por el alumno mostrando su originalidad, como resultado del estudio de la normatividad, de la jurisprudencia y de la doctrina relacionada con los delitos informáticos que se vienen presentado a raíz del desarrollo de esta nueva tecnología, que a su vez es muy importante empezar a recopilar las distintas normatividades desarrolladas en el derecho comparado con nuestras normas colombianas para ponernos a tono con el pensamiento globalizado y tener claridad con los distintos delitos que van surgiendo con el trasegar de estas nuevas tecnologías.

La formulación del problema es clara y se encuentra delimitado en el tiempo y en el espacio. Los fundamentos teóricos de la investigación están sustentados en la Ley, la Doctrina y la Jurisprudencia, se dio cumplimiento a los objetivos propuestos en el proyecto de investigación, es comprensible la terminología sobre los nuevos delitos informáticos que cada día se están presentando y que se deben ir tipificando en nuestra legislación.

El trabajo de doctor González es significativo desde todo punto de vista por estar acorde con la realidad jurídica colombiana, estamos seguros de que será una valiosa obra y texto de consulta por cuanto encierra el complejo mundo de los delitos informáticos, que expone con sencillez y agradable interés, el cual será muy atrac6tivo por ser un tema que necesariamente tenemos que saber y ejercer, los que estamos comprometidos con el Derecho Penal.

Por lo anterior considero que los objetivos propuestos en el trabajo de investigación se han cumplido, lo cual justifica mi **APROBACION** para seguir con el procedimiento académico reglamentario y pueda otorgársele el merecido título de **Magíster en Derecho Penal**.

Atentamente,

JOSE EDUARDOSAAVEDRA ROA

LOS DELITOS INFORMATICOS Y SU APLICACION EN LA LEGISLACION COLOMBIANA

JOSE JOAQUIN GONZALEZ CARRILLO

UNIVERSIDAD LIBRE DE COLOMBIA
FACULTAD DE POSTGRADOS
MAESTRIA EN DERECHO PENAL
BOGOTÁ
2010

LOS DELITOS INFORMATICOS Y SU APLICACION EN LA LEGISLACION COLOMBIANA

JOSE JOAQUIN GONZALEZ CARRILLO

UNIVERSIDAD LIBRE DE COLOMBIA
FACULTAD DE POSTGRADOS
MAESTRIA EN DERECHO PENAL
BOGOTÁ
2010

NOTA DE ACEPTACIÓN

_____

_____

PRESIDENTE DEL JURADO

_____

JURADO

_____

JURADO

_____

_____	_____	_____	_____
CIUDAD	**DIA**	**MES**	**AÑO**

TABLA DE CONTENIDO

Pág.

INTRODUCCION

Esta monografía, pretende ser una referencia dentro del contexto de los delitos informáticos y cuyo objetivo es ponernos a tono con los avances tecnológicos y la penalización del mal uso de estos recursos.

En Colombia, hasta ahora se le está dando la importancia y la atención de crear la normatividad jurídica de los delitos informáticos en vista de la cantidad de delitos que se están suscitando a través de la red tales como, apología del genocidio, el homicidio, lesiones personales, acceso no autorizado a sistema de procesamiento de datos, abuso de confianza informática, daño informático, extorsión informática, sabotaje informático, espionaje informático, hurto informático, falsedad informática, estafa informática, corrupción de menores vía informática, ofrecimiento engañoso de productos y servicios, pánico económico, terrorismo entre otros, delitos éstos que se han ido creando a través de las nuevas tecnologías y que precisamente el Estado como garante de la vida, honra y bienes de los ciudadanos le ha correspondido empezar a legislar y a crear su propia jurisprudencia con el fin de combatir estas conductas y restablecer el derecho a las personas naturales y jurídicas lesionadas.

Iniciamos este estudio desde la perspectiva del derecho penal para analizar los delitos mediante las computadoras y sus implicaciones criminológicas, ya que el hombre a través de la tecnología ha creado máquinas y sistemas que lo ayuden a la automatización de la información, los procesos informáticos y en general las comunicaciones pero durante este proceso nunca se planeó que la automatización informática generara una infinidad de comportamientos antijurídicos apartados de las formas tradicionales. De modo tal que la normatividad penal vigente no era suficiente para regular estos comportamientos, lo cual ha llevado a estructurarse de un modo comparativo entre legislaciones de los países que afrontan esta problemática informática-jurídica.

En Colombia, en opinión de la doctrina tradicional, no se ha tipificado en su totalidad, la generalidad de estas conductas delictivas. Por consiguiente nuestro objetivo es realizar una valoración de la legislación colombiana frente a tales comportamientos sobre todo en lo que la doctrina penal conoce como tipicidad y que en una próxima reforma debemos ajustarnos a los parámetros internacionales teniendo en cuenta una adecuación legislativa acorde con la problemática nacional y en la cual no se dejen de lado temas pertinentes a cada conducta.

Presento en este trabajo, lo correspondiente a antecedentes en el derecho colombiano y otras legislaciones, como una propuesta novedosa y actual en un mundo tecnificado como el actual a través del Internet, medio por el cual nos entrelazamos ante el mundo, pero que también ha dado pie para que personas inescrupulosas que se apartan de los parámetros de la ley los utilicen valiéndose del anonimato para la comisión de estos nuevos delitos.

Lo que he pretendido con este trabajo es que el Estado, las Universidades, los juristas y abogados y las demás personas del común, tengamos conocimiento de la existencia de estos delitos y que el legislador se encargue de tipificar cada uno de dichos delitos para que no se vulnere los derechos de las personas tanto naturales y jurídicas nacionales e internacionales ya que la red involucra a todos los países del mundo. De igual manera, que las Universidades continúen el estudio y desarrollo de estas investigaciones ya que la tecnología avanza vertiginosamente y países como el nuestro no se pueden quedar a la zaga en esta clase de delitos.

1. EL PROBLEMA DE INVESTIGACION.

¿Teniendo en cuenta que los avances tecnológicos como el sistema en red y la Internet han generado una infinidad de comportamientos antijurídicos, será que la normatividad penal colombiana hasta el momento ha regulado plenamente estos delitos informáticos?.

1.2. HIPOTESIS

Es necesario que el legislativo tipifique la generalidad de los delitos informáticos para que no queden vulnerados los derechos de las personas naturales y jurídicas y quedar en consonancia con legislaciones jurídicas de otros países desarrollados, con el fin de combatir las altas cifras de criminalidad, a través de las distintas etapas en el desarrollo del proceso de investigación, haciendo más explícito el concepto de información y su importancia en el ámbito jurídico, teniendo claridad en la noción de delito y con ella la relación que existe entre los elementos que componen al delito y la información con especial relevancia a las clasificaciones propuestas por la doctrina nacional e internacional.

1.3. JUSTIFICACION

El hombre ha evolucionado y con el ha surgido la capacidad de crear medios para conseguir efectivamente los fines y propósitos en actividades tan cotidianas como lo es el comercio para lo cual ha desarrollado la inminente necesidad de crear herramientas para hacer menos engorrosas las actividades que cada vez son más complejas en el normal acontecimiento del progreso del hombre, su entorno y sus actividades.

Como consecuencia del desarrollo tecnológico digital que vive el mundo actual, ha nacido el mundo informático o ciberespacio, producto del avance de los medios de información e interconexión global, siendo un elemento de gran despliegue en todos los campos; no solo es una gran red de información y comunicación, sino que además es el sitio ideal para poder ejercer la actividad comercial puesto que a través de ella se pueden realizar negocios jurídicos con la utilización de medios electrónicos.

La Internet, novedosa herramienta que ha contribuido a dar un paso significativo en la elaboración de operaciones comerciales sin duda alguna es, el motor que lleva las riendas del comercio electrónico. La Internet definida como el conjunto de redes interconectadas globalmente que crean un modo de que la comunicaciones puedan ser realizadas sincrónicamente desde un equipo cualquiera en interconectividad con la red, con otros servidores que participan interactivamente en la misma red; éste sistema de interconexión global se encuentra unido por lugares de direcciones de sitios Web. Dicha herramienta hoy

en día se encuentra en todos los escenarios y no se puede ignorar el empuje que su uso comercial le ha dado al desarrollo mercantil y del mundo de los negocios.

Sin embargo a pesar de lo conveniente que resulta hacer uso de los medios informáticos para la práctica del comercio, el manejo de tales herramientas ha generado que personas inescrupulosas y delincuentes utilicen estas vías para afectar a las personas naturales y jurídicas circunstancias por las cuales le ha correspondido al Congreso legislar sobre conductas ilícitas como, el ofrecimiento engañoso de productos y servicios, el pánico económico, el lavado de activos y la omisión de control, el daño informático, la extorsión informática, sabotaje informático, espionaje informático, acceso no autorizado a sistema de procesamiento de datos, abuso de confianza informática, hurto informático, falsedad informática, estafa informática, corrupción de menores vía informática, lo que se pretende es retomar el derecho comparado de la experiencia de los países europeos y de Estados Unidos entre otros, para lograr armonizar y proyectar un nuevo Código Penal quien es el competente para conocer e investigar dichos delitos.

De manera tal, que esta nueva gama de hechos punibles corresponde a un conjunto de conductas tipificadas que atentan contra distintos objetos jurídicos y cuyo fin material y productivo es la información, razón por la cual es menester que nuestro Código incluya todos aquellos comportamientos en los que intervienen en su comisión como herramienta del delito, las tecnologías informáticas.

1.4. OBJETIVOS

1.4.1 OBJETIVO GENERAL

Plantear que con el desarrollo de la alta tecnología informática como los sistemas en red y la Internet, se han originado conductas delictivas que deben ser tipificadas en una nueva reforma al Código Penal, con el fin de que no se sigan vulnerando los derechos de las personas naturales y jurídicas, nacionales e internacionales.

1.4.2 OBJETIVOS ESPECIFICOS

- Establecer los elementos jurídicos con los que cuenta la legislación Colombiana para la penalización de los delitos informáticos.

- Determinar cuáles son las políticas nacionales e internacionales existentes para la penalización de dichos delitos.

- Estudiar las distintas conductas antijurídicas relacionadas con la informática para así lograr una clara tipificación y penalización de las mismas.

- Entrar en consonancia con países desarrollados que tengan amplia experiencia en el tema jurídico de éstos delitos para alcanzar la unificación jurídica universal.

- Ilustrar sobre la evolución que ha tenido la informática y su desarrollo jurídico a fin de establecer los delitos que con dicha práctica se han generado.

- Dar a conocer algunas conductas delictuales que se generan con la nueva tecnología informática.

- Establecer análisis juridisprudencial en materia de delitos informáticos con el fin de lograr combatir a las personas inescrupulosas que utilizan estos medios de manera delictual.

2. MARCO TEORICO

2.1. ANTECEDENTES HISTÓRICOS

2.1.1. Historia de la informática y la comunicación en un mundo globalizado.

La actividad comercial, tradicionalmente se ha ejercido de manera personal y con las formalidades propias de los respectivos tipos de documentos y los elementos de formación de los diferentes contratos mercantiles, pero con la evolución, transformación, industrialización y globalización en el marco mundial ha surgido durante las últimas décadas en el campo informático una gradual globalización cibernética, que marca el sendero hacia nuevas tecnologías que constituyen mecanismos y herramientas eficaces y eficientes para lograr un acercamiento y un avance significativo en las comunicaciones mundiales, lo cual implica un acercamiento real y práctico en las relaciones en escenarios de la actividad humana.

Las tecnologías de la información han tenido un papel protagónico desde finales del siglo XIX hasta nuestros días, marcando una gran influencia en los sectores económicos, jurídicos y sociales, es así que algunos estudiosos como DANIEL BELL[1] en 1973 tituló su obra *"El advenimiento de la sociedad posindustrial",* ZBIGNIEW BREZEZINSKI[2] en 1973 *"La era tecnológica",* MANUEL GARCIA

[1] BELL, Daniel, El advenimiento de la sociedad posindustrial, Madrid, Edit Alianza, 1976.
[2] BREZEZINSKI, Zbigniew, La era tecnológica, Buenos Aires, Edit Paidós, 1973.

PELAYO[3] en 1974 *"Burocracia y tecnocracia y otros escritos".* En 1948 SHANON[4] publicó su estudio "*Mathemetical theory of comunication"* en el cual formuló los principios matemáticos que aún sustentan la teoría de la información. En el mismo año Norbert Wierner en su obra *"Cybernetics"* o sea la nueva ciencia de la comunicación y control entre el hombre y la máquina, resalta la importancia de las comunicaciones en las diferentes ciencias, en la sociedad y en la esfera jurídica[5].

Al respecto el jurista Abelardo Rivera Llano sostiene: "…Si la cibernética que ha comenzado lo que muy bien se ha llamado la segunda revolución industrial, entendida en última instancia, como ciencia de la eficacia, de la acción, ha ido penetrando e invadiendo todos los campos del quehacer humano de donde la eficacia, que es su consecuencia la cual exige procedimientos rápidos, ágiles y flexibles, se ha convertido en el eje rector del mundo que ve, de una parte multiplicarse vertiginosamente las relaciones humanas en virtud de las nuevas y dinámicas formas de comunicación –telemática entre otras- que la complejidad de la vida actual y de la sociedad de masas, solo puede reducirse mediante el aporte de las leyes cibernéticas (concretamente, de la termodinámica) y sus aplicaciones tecnológicas, propias de la informática. Y, el derecho como producto social que es, no podía estar ausente de su influencia, efectos y repercusiones, como que es, por esencia, un medio de control social directo.

[3] GARCIA PELAYO, Manuel, Burocracia y tecnocracia y otros escritos, Madrid Edit Alianza, Fondo de la Cultura Económica, 1974.
[4] SHANON, Claude E., A mathematical theory of comunication, en Bell System Tecnical Journal 27 (1948), citado por CROSSON, Frederick y SAIRE, Kenneth, Filosofía y Cibernética, México, Fondo e la Cultura Económica, 1982.
[5] Wierner, N. Cybernethic,. Cambridge. Mass: M.I.T. Press, 1948, citado por CROSSON, F.y SAIRE, K, Filosofía y Cibernetica, México, Fondo de la Cultura Económica, 1982.

Con ello se quiere decir que la actividad jurídica puede entenderse como un sistema que reacciona con regulaciones (*output),* a las perturbaciones *(input)* procedentes de su medio social…"[6]

A finales de los años setenta y principios de los ochenta, teniendo como base dichos estudios, se llegó a importantes conclusiones tales como el significativo incremento de la producción en el sector servicios en relación con otros sectores reales de la economía, generando un flujo de capitales del sector industrial al sector servicios. De igual manera, la educación tuvo un viraje trascendental, las universidades dieron mayor relevancia a ciencias como la estadística y la econometría y con la certeza de que la información técnica era un elemento fundamental para la toma de decisiones económicas, los dueños de los medios de producción comenzaron a acaparar tales "bienes informáticos",[7] razón por la cual a comienzos del siglo pasado se creó el "computador electrónico", una de las tecnologías de la información que cambiaría radicalmente el proceso de almacenamiento, catalogación y recuperación de información; así mismo se crearon las bases de datos facilitando el cotejo de la información.

Sin embargo, las críticas de los detractores, sobre el manejo que se estaba dando a las nuevas tecnología no se hicieron esperar, ya que vieron en las computadoras y en dichas bases de datos una amenaza a la intimidad e incluso contra la democracia pues este evolucionado invento fortalecía la vigilancia estatal, además se ejercía un control estricto para el pago de tributos y nuevos impuestos comerciales.

---

[6] RIVERA LLANO Abelardo. Dimensiones de la informática en el derecho. Perspectivas y problemas. Editorial Jurídica Radar. Bogotá 1985. Pág 2

[7] MARQUEZ ESCOBAR, Carlos Pablo. El delito informático. La información y la comunicación en la esfera penal conforme con el nuevo Código Penal. Bogotá. Ed. Leyer. Pág 72.

Con el advenimiento de las nuevas tecnologías, paulatinamente el tiempo y la distancia han dejado de ser limitantes para efectuar operaciones mercantiles; los contenidos de información, publicidad, mercadeo ahora pueden ser dirigidos de manera masiva en busca de una cobertura global.

En éstas nuevas formas de acercamiento e integración global encontramos inmerso al comercio, el cual ha encontrado que estos mecanismos y herramientas han sido fundamentales para dar a conocer y poner a disposición de los consumidores los diferentes tipos de mercancías, las cuales son ofrecidas desde cualquier lugar del mundo, rompiendo todo tipo de fronteras que imposibiliten ofertar las mercancías o demandar las mismas.

"El proceso operativo de transacción comercial en la cual las partes participantes no interactúan de manera personal, ni por medio de representantes ni de agentes comerciales, sino que logran llegar a un acuerdo comercial de manera electrónica, es decir en el entendido de este término, a los medios como la Internet, la televisión, el teléfono entre otros, se conoce como comercio electrónico"[8].

El comercio electrónico no se trata de una novedad, su aparición se da varios años atrás, se produce una revolución desde la presencia de computadores en las empresas, y se crea un sistema de intercambio electrónico de información comercial con la invención del EDI (Intercambio Electrónico de documentos); y desde entonces ha sido ejercido por medio de redes privadas y públicas reguladas por códigos o acuerdos en el contexto de EDI.

[8] ORGANIZACIÓN MUNDIAL DEL COMERCIO, Estudios Especiales 2. El Comercio Electrónico y el papel de la OMC. Instrumentos del Comercio Electrónico.

Las relaciones comerciales realizadas mediante el uso de una computadora para transmitir datos y el intercambio de los mismos, se da a principios de la década de los 70. Este innovador sistema de información contribuyó con adelantos en los procesos de fabricación en el ámbito privado, entre empresas de un mismo sector. Hacia la mitad de la década de los 80, con el favor de la televisión, surgió una nueva forma de venta directa, conocida como venta por catálogo. De esta manera, los productos eran exhibidos con mayor realismo, y los pagos de los productos eran realizados a través de las tarjetas de crédito.

El IED se utilizaba en sistemas de tipo radial entre grandes fabricantes y sus proveedores. Sus miembros se integraban en una red que contaba con infraestructura propia de telecomunicaciones y formatos normalizados, pero sus altos costos de equipo y de conexión limitaban su difusión. Estos fueron los primeros pinos hacia lo que hoy conocemos como intercambio electrónico de datos.

La Asamblea General de la Organización de las Naciones Unidas (ONU[9]), solicitó a la Comisión para el Derecho Mercantil Internacional-CNUDMI- ser el órgano encargado de redactar una normatividad que regulara todo lo referente a la materia del comercio electrónico y que a su vez ésta cumpliera con la función de servir de referente para que los países la adoptaran en sus respectivas legislaciones, teniendo en cuenta que la industria de las telecomunicaciones ha tenido un alto índice de crecimiento en razón a que el hombre actual vive y se desarrolla en un medio donde los datos, la información y la comunicación son parte fundamental de la vida diaria. La información se desempeña como el “bien”

[9] Por medio de la Resolución 51/162 de 1996

que las organizaciones capitalistas más valoran por su potencialidad para generar un mayor desarrollo económico[10].

Así, la globalización que tiene un carácter multidimensional abarca diferentes campos como el económico, el tecnológico, el político y el cultural. En este sentido el Fondo monetario Internacional F.M.I. la define como una interdependencia económica creciente del conjunto de países del mundo provocada por el aumento del volumen y la variedad de las transacciones transfronterizas de bienes y servicios, como de los flujos internacionales de capitales, simultáneamente con la difusión acelerada de la tecnología.

2.2. Definición y concepto de tecnología y formas de comunicación.

Informática es la ciencia aplicada que abarca el estudio y tratamiento automático de la información, utilizando dispositivos electrónicos y sistemas computacionales. También está definida como el procesamiento automático de la información.

En la informática convergen los fundamentos de las ciencias de la computación, la programación y metodologías para el desarrollo de software, la arquitectura de computadores, las redes de computadores, la inteligencia artificial y algunos elementos relacionados con la electrónica, entendiéndose como la unión sinérgica de este conjunto de disciplinas, una de la aplicaciones más importantes de la informática es proveer información en forma oportuna y veraz, facilitando tanto la toma de decisiones a nivel gerencial como permitiendo el control de procesos críticos.

[10] MARQUEZ ESCOBAR. El delito informático. La información y la comunicación en la esfera penal, conforme con el Nuevo Código penal. Pág 19

El vocablo *informática* proviene del francés *informatique*, acuñado por el ingeniero Philippe Dreyfus para su empresa «Société d'Informatique Appliquée» en 1962. Pronto aparecieron adaptaciones del término en italiano, español, rumano, portugués y holandés, entre otros, para hacer referencia a la aplicación de las computadoras para almacenar y procesar la información.

En el Diccionario de la Real Academia Española se define *informática* como:

"El conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".

Conceptualmente, se puede entender como aquella disciplina encargada del estudio de métodos, procesos, técnicas, desarrollos y su utilización en ordenadores (computadoras), con el fin de almacenar, procesar y transmitir información y datos en formato digital.

Según el CONPES, las Tecnologías de la comunicación las define como herramientas que permiten el desarrollo de una nueva economía, la construcción de un Estado más moderno y eficiente, la universalización del acceso a la información y la adquisición y utilización eficaz del conocimiento, elementos fundamentales para el desarrollo de una sociedad moderna. El documento CONPES 3072 de 2000 hace un diagnóstico de la incursión del país a los procesos de modernización y la productividad relacionados con las tecnologías de la información y así mismo señala un plan denominado "Agenda de Conectividad", la cual está orientada a impulsar el desarrollo socio-económico del país, masificando el uso de las Tecnologías de la Información y la Comunicación TICs a fin de maximizar la eficiencia y transparencia básicamente en la gestión pública.

La utilización de las Tecnologías de Información y Comunicación (TIC's)[11], ha sido relevante en la influencia de un nuevo modo de información, comunicación y por su puesto también de comercio, lo que ha generado agitación en el mundo jurídico.

El término comercio electrónico abarca todos aquellos asuntos originados por las relaciones de índole comercial, contractuales o no, constituidas a partir del uso de uno o más mensajes de datos o de cualquier otro medio semejante. La ley 527 de 1999 describe las relaciones de índole comercial[12] sin forjar una limitación de ellas; entre estas se encuentran las operaciones comerciales de suministro o intercambio de bienes o servicios; acuerdos de distribución; operaciones de representación o mandato comercial; operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; acuerdos de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o

[11] http://es.wikipedia.org/wiki.TecnologíasdeInformaciónyComunicación´s//

[12] Ley 527 de 1999 Articulo 2º. *Definiciones*. Para los efectos de la presente ley se entenderá por:
a) **Mensaje de datos.** La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;
b) **Comercio electrónico.** Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar.
c) **Firma digital.** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;
d) **Entidad de Certificación.** Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;
e) **Intercambio Electrónico de Datos (EDI).** La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto;
f) **Sistema de Información.** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera.

El comercio electrónico hace referencia a las operaciones mercantiles llevadas a cabo mediante sistemas electrónicos de procesamiento y transmisión de información. Las principales herramientas para lograr este cometido son la utilización de EDI (*Electronic Data Interchange*), conocido también como el intercambio de mensajes electrónicos, el cual se basa en la transmisión electrónica de datos de una computadora a otra, se encuentra estructurado bajo normas técnicas convenidas al efecto; y la Internet *(Interconnected networks),* entendido como un sistema global de información que se encuentra interconectado por un espacio global de direcciones, el cual se encuentra en condiciones de sobrellevar comunicaciones en gran masa, brindando así el uso y acceso a la red global.

Según el autor David Kosiur[13] : "Comerció Electrónico es un sistema que incluye no sólo aquellas transacciones que se centran en la compra y venta de bienes y servicios para generar ingresos, sino también aquellas transacciones que respaldan la generación de los ingresos, tales como la creación de la demanda para esos bienes y servicios, ofreciendo respaldo a las ventas y el servicio al cliente, o facilitando la comunicación entre socios de negocios".

Ernesto Rengifo García[14], define comercio electrónico, como: "...el intercambio de información entre personas que da lugar a una relación comercial, consistente en la entrega en línea de bienes intangibles o en un pedido electrónico de bienes tangibles. Este intercambio de datos puede ser "multimedia" o consistir en imágenes, textos y sonidos."

[13] KOSIUR David**,** Understanding Electronic Commerce. Redmon. Press. 1997. Página 4.
[14] RENGIFO GARCÍA Ernesto, Nuevos Retos del Derecho Comercial, Comercio Electrónico, Documento Electrónico y Seguridad Jurídica, Primera edición, Biblioteca Jurídica Dike, 2000, Pág. 212.

Por su parte, Carlos Vattier Fuenzalida[15], tratadista español afirma que "... los contratos electrónicos son los que se celebran mediante el llamado dialogo de ordenadores, el cual discurre entre el ordenador del emisor y el ordenador del receptor a través de una red telemática binaria interactiva de operadores intermedios, cuya más lograda expresión actual es la popular red Internet."

Lo cierto, es que el comercio electrónico y los TIC´s, son una valiosa herramienta para el ejercicio de operaciones comerciales, sin el establecimiento de un contacto personal de las partes en cuestión.

Las relaciones comerciales se pueden efectuar mediante un sistema cerrado y un sistema abierto.

Sistema cerrado se refiere al intercambio electrónico de datos llevado a cabo entre un grupo de participantes limitado; dicho intercambio comúnmente es realizado a través de redes públicas o privadas que funcionan bajo normas técnicas previamente acordadas por los participantes y reguladas por códigos o por acuerdos. La adopción de este tipo de acuerdos promueve la seguridad jurídica de quienes participan en las transacciones, al tiempo que respeta las formas de acceso y seguridad de la red, así como la plena validez de las operaciones que se realicen a través de la misma, este es el caso del EDI (intercambio electrónico de datos) y la intranet[16].

Caso contrario es la Internet que es un sistema abierto de comunicación entre ordenadores, el cual posee una estructura abierta, descentralizada con una cobertura que no se encuentra restringida a determinado tipo de usuarios, es

[15] Vattier Fuenzalida Carlos, Instituciones del Derecho Privado – Contratación Contemporánea, Palestra editores Lima– Editorial Temis S.A. Bogotá, 2001, Pág. 20.

[16] Intranet es una red privada que se basa en las mismas tecnologías que Internet, pero que se encuentra restringida para el uso de un grupo de usuarios determinado.

multidireccional en su interactividad, realizando una interconexión en red con todas las demás redes informáticas de cualquier lugar; además, cuenta con un número ilimitado de participantes, a diferencia de los sistemas cerrados en los cuales la participación es limitada.

Realmente, no existe una definición formal de la Internet, solo se trata de una red de redes internacional y pública, la cual tuvo su origen en los años 60s cuando los militares norteamericanos establecieron una red entre sus sitios de trabajo académico ("research") con tal éxito que ha alcanzado los niveles de masificación del uso de este medio y la comercialización que hoy conocemos.

Sin embargo, ninguna entidad es dueña de Internet, ni la controla; las redes nacionales funcionan según políticas nacionales y enlaces internacionales, según acuerdos entre compañías proveedoras de servicios de telecomunicaciones, las cuales junto con los gobiernos, las corporaciones internacionales y las universidades comparten el control de Internet. Las compañías proveedoras del servicio son las dueñas de buena parte de la infraestructura física, los proveedores del servicio de Internet son los dueños de los servidores, las universidades de los sistemas críticos sin los cuales Internet dejaría de funcionar, y los particulares o compañías privadas son los titulares de los derechos de propiedad intelectual de la información enviada, almacenada o publicada en la red.

3.DERECHO COMPARADO SOBRE LA INFORMATICA

A diferencia de los Estados Unidos, donde prima la política de auto-regulación de los particulares, respecto a la privacidad, en Europa se ha adoptado una conducta diferente, es así como el proyecto de Directiva sobre Privacidad en la Información *(Data Privacy Directive)* prohíbe la transferencia de información sobre ciudadanos de la Unión a países que no tengan una reglamentación que garantice la protección de la información[17]

En 1996 la Unión Europea promulgó la Directiva para la Protección Legal de Bases de Datos *(EU Directive on the legal Protection of Databases),* la cual impuso la obligación de promulgar leyes para la protección de bases de datos, las cuales define como: *"la recopilación de trabajos independientes, información u otros materiales organizados en forma sistemática o metódica e individualmente asequible ya sea mediante medios electrónicos o de otro tipo"*[18]*.*

Dicha Directiva protege las bases de datos de la substracción de información no autorizada hasta por un término de 15 años, independientemente de que reúnan los requisitos para ser objeto de protección de derechos de autor. Adicionalmente, la Directiva establece para los titulares de bases de datos no europeos un requisito de reciprocidad con el cual se le niega la protección a las bases de datos creadas en países por fuera de la Unión Europea.

[17] BOTERO, CONCHA, CABALLERO, GODOY, MONTGOMERY, PARDO, Comercio electrónico en Colombia. Principales aspectos legales. Bogotá. Editor Raisbeck, Lara, Rodríguez & Rueda (Baker & McKenzie) 2002. Pág 61.

[18] BOTERO, CONCHA, CABALLERO, GODOY, MONTGOMERY, PARDO, Op. Cit. Pág 62.

Tras amplias discusiones y negociaciones la Comisión Europea y el Departamento de Comercio de los Estados Unidos lograron el 14 de marzo de 2000 un acuerdo sobre la forma en que las compañías estadounidenses puedan cumplir con la Directiva, para poder operar en territorio europeo, adoptando unos parámetros llamados los *Safe Harbor Principles,* donde las empresas deben notificar a los usuarios sobre el propósito de la recolección de información, debe dar al usuario la posibilidad de determinar o evitar que su información sea divulgada a un tercero, debe dar la posibilidad de solicitar su corrección, modificación o eliminación total cuando esta sea inexacta, la información recogida debe ser relevante para el propósito para el cual está siendo recopilada.

A raíz de los atentados perpetrados el 11 de septiembre de 2001 en Nueva York, el presidente Bush solicitó al Parlamento Europeo la modificación del proyecto de Directiva de Privacidad con el fin de permitir que las ISPs *(Internet Service Providers)* retengan información enviada o consultada por los usuarios en un término prudencial a fin de que las agencias de seguridad la revisen y adopten medidas si se tiene sospecha de que la información este siendo utilizada para fines terroristas u otros ilícitos[19].

Con respecto a la privacidad en comunicaciones por medios electrónicos entre particulares en Estados Unidos, se encuentra parcialmente regulada por el ECPA *(Electronic Communications Privacy Act,* el cual determina algunas obligaciones a quienes procesan y manejan comunicaciones electrónicas y a quienes interceptan tales comunicaciones, cubriendo aspectos tales como:

- Privacidad e los flujos de comunicación.

[19] Journal The Economist, Markets for ideas. Marzo 2010 LSSI and Notice.

- Prohibición a los proveedores de servicios de comunicación electrónica la divulgación intencional de información a persona diferente del remitente y el destinatario de la información.
- Regulación de lo relacionado con la privacidad sobre la información almacenada en forma electrónica.
- Prohibición a los proveedores de servicios de comunicaciones electrónicas que presten servicios al público, la divulgación de la información almacenada en forma electrónica. A los sistemas privados no los cubre esta prohibición.

En Estados Unidos una ley que se ocupa de la privacidad en las comunicaciones electrónicas es el CFAA *(Computer Fraud and Abuse Act),* que prohíbe obtener información relativa a la seguridad nacional de los Estados Unidos, cuando se tenga motivos para creer que existe la intención de usarla contra los intereses de los Estados Unidos. Igualmente prohíbe obtener información de los archivos de las instituciones financieras, las centrales de riesgo y los emisores de tarjetas de crédito en forma intencional.

Con el fin de contrarrestar la acción de los intrusos *(hackers),* fue expedido en los Estados Unidos el *Nacional Information Infrastructure Protection Act,* ley que protege los archivos e información de instituciones financieras e información interestatal e internacional emitida por computador[20]. Cabe anotar que el uso de servidores y software anticuados por parte de ISPs *(Internet Service Providers)* y de los operadores de los sitios han facilitado a los *hackers* la toma de información en forma ilícita.

El caso de la empresa vendedora de CDs por Internet, CD Universe, donde un *hacker* dijo a la empresa que tenía acceso a los archivos electrónicos de la

[20] BOTERO, CONCHA, CABALLERO, GODOY, MONTGOMERY, PARDO, Op. Cit. Pág 53.

compañía obteniendo los nombres y números de tarjetas de crédito de por lo menos 530.000 tarjetahabientes, por lo cual exigió una gran suma a la compañía para abstenerse de colocar la información en un sitio de acceso público y ante la negativa de la compañía el *hacker* exhibió los nombres y tarjetas de crédito de los miles de tarjetahabientes en un sitio de la red, es así como la información personal de los navegantes es un activo susceptible de ser vendido.

De otra parte, debido a la preocupación de los padres en los Estados Unidos, por la información obtenida por los navegantes menores, en 1998 se expidió el *Children´s Online Privacy Protection Act,* que obliga a todos los sitios que recojan información de menores de 13 años, solo sea con el consentimiento de los padres. La ley establece que el consentimiento de los padres debe ser "verificable" pero no establece los mecanismos para este fin[21].

En noviembre de 2001 el Parlamento Europeo aprobó una reforma a la Directiva de Privacidad de la Unión Europea con el fin de restringir el uso del *spam* (correo publicitario y promocional no solicitado), las *cookies* (pequeños archivos de texto colocados por el servidor del sitio visitado en el *hard drive* del computador del visitante, que contiene información sobre el idioma que habla, las páginas que visita, e información adicional), y otros mecanismos de rastreo de usuarios.

Otro aspecto preocupante con respecto a la privacidad en la red, se refiere a los software desarrollados por los servicios de inteligencia de los Estados Unidos, para monitorear las comunicaciones en el ciberespacio, como son, Echelon, Carnivore y el Magic Lantern el cual graba toda la información que teclee un usuario en su computador sin que se de cuenta y luego envía ilegalmente dicha

[21] Journal The Economist, Markets for ideas. Marzo 2010 LSSI and Notice.

información a la respectiva agencia de inteligencia por Internet, ésta amenaza a la privacidad de las personas ha generado controversia a nivel mundial, especialmente en la Unión Europea[22]. Algunas cortes de los Estados Unidos han manifestado que un acuerdo entre una persona y un ISP (Internet Service Provider) no se puede considerar como libremente negociado.

La Corte Federal de Distrito de los Estados Unidos, apoyada en la Primera Enmienda de la Constitución, produjo un fallo el 7 de noviembre de 2001, donde declara sin vigencia ni fuerza vinculante una providencia emitida por una corte francesa el 20 de mayo de 2000 donde se ordena a Yahoo Inc: eliminar el posible acceso de los ciudadanos franceses a todo material en el sitio de subasta de Yahoo.com que ofrezca objetos, reliquias, insignias, emblemas y banderas nazis; eliminar el acceso de ciudadanos franceses que muestren textos, extractos o citas de Mi Lucha y el Protocolo de los Ancianos de Zion; ante lo cual Yahoo acudió a la Corte Federal de Distrito de los Estados Unidos, que manifestó en su fallo que dado que no existe un convenio internacional que establezca los estándares internacionales aplicables a la Internet, prima la obligación de la Corte de hacer cumplir la Primera Enmienda de la Constitución de los Estados Unidos sobre el principio de la reciprocidad en el cumplimiento de las providencias judiciales extranjeras. Como vemos, han existido muchos obstáculos para la reglamentación del uso de la Red por parte de los estadounidenses y no han dejado tutelar la evolución tecnológica de la Red.

En cuanto a la evolución legal de Internet en países centroamericanos como el Salvador, declara mediante el decreto 554 de 18/ 06/ 1997 de *"interés nacional el acceso a la red Internet para todos los habitantes del territorio nacional, en*

[22] BOTERO, CONCHA, CABALLERO, GODOY, MONTGOMERY, PARDO, Op. Cit. Pág 58.

condiciones sociales y geográficas equitativas, con tarifas razonables y con parámetros de calidad acordes a las modernas aplicaciones de la multimedia[23]".

Así mismo el artículo 14 de la Constitución del Salvador dispone: *Todos los habitantes gozan de derechos tales como la publicación de sus ideas por prensa sin censura previa…", artículo 32: "no se dictarán normas que restrinjan la libertad de imprenta"* finalmente el articulo 42 de la misma Constitución prescribe *"las autoridades proveerán a la protección de…los derechos a los usuarios y consumidores…"*

Dichos artículos sirvieron de fundamento al Decreto 1279 de 1997 donde *"Se declara que el servicio de Internet, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión correspondiéndole en tal sentido las mismas consideraciones que a los demás medios de comunicación social".*

Es tal la importancia que le ha dado este país a la red de comunicaciones que ha elevado a rango de constitucional el uso del servicio de Internet y además declaró de interés general el acceso a la red.

Uso ilegítimo de un Terminal de telecomunicaciones. Artículo 256 C.P. Español[24].

Artículo 256 C.P: "El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, (300,51 Euros), será castigado con la pena de multa de tres a doce meses".

[23] http://www.salvador.edu.ar/castoldi.htm. Aspectos legales derivados de la Implementación de Sistemas Informáticos. Pág 1-4, 26 de mayo de 2003

[24] http://es.wikipedia.org/wiki/November 2006 Defraudaciones and Telecomunicaciones/

Este artículo regula lo que la doctrina denomina Uso no autorizado o utilización abusiva de equipos terminales de telecomunicaciones. Si el perjuicio es inferior a 300,51 Euros, supone una falta del artículo 623 C.P (faltas contra el patrimonio).

Aquí no hay transmisión de la propiedad, ni siquiera no lo aprehensible, solamente una persona utiliza lo que es de otro.

Objeto: Terminal de comunicación: Cualquiera cuyas características sirvan para establecer una comunicación a distancia entre las personas, sistemas o entre dispositivos técnicos, mediante procedimientos eléctricos, informáticos, telefónicos, etc.

La doctrina intentó acotar este concepto, y determinaron que no entra en el mismo los aparatos que sirvan para procesar datos, por lo tanto, no se incluye el uso del ordenador cuando esté conectado a una red local. Es necesario que el sistema sea un auténtico terminal, que permita interconectar distintas comunicaciones. Un terminal de telecomunicaciones es algo más que un teléfono móvil.

Acción: Recoge dos conductas:
- Uso no autorizado.
- Uso distinto al autorizado.

Bien jurídico protegido: Es el patrimonio individual del titular del equipo de telecomunicaciones. No se exige un ánimo especial para cometer este delito.

Sujeto activo:

- Puede ser cualquiera, por ejemplo, un empleado que va más allá de la utilización autorizada por la empresa.

- Cualquier tercero que acceda al Terminal y lo maneje sin autorización.
- Un tercero que desde otro ordenador accede a un equipo terminal y lleve a cabo un uso no autorizado.

Modalidad: El Phreaking telefónico y el artículo 256 C.P:

La manipulación no se produce directamente sobre la red telefónica, sino que se utiliza directamente el terminal de telecomunicaciones para llevar a cabo la defraudación.

Cierre de páginas webs: ¿Futura ley reguladora de la descarga de contenidos no autorizados?[25]

El Gobierno ha elaborado un Anteproyecto de Ley denominado ANTEPROYECTO DE LEY DE ECONOMÍA SOSTENIBLE que pretende ser, entre otras cosas, la futura ley reguladora de las descargas de contenidos no autorizados en la Red.

A través de esta Ley se pretende impulsar la industria española de contenidos y articular mediante un mismo documento todos los proyectos del Gobierno ideados para contrarrestar los efectos de la crisis.

Análisis

La Disposición Final Primera del Anteproyecto, se organiza de la siguiente manera:

- Apartados 1º y 2º: Modifican la Ley 34/2002 de Servicios de la Sociedad de la Información y del comercio electrónico. (en adelante LSSI)

[25] Journal The Economist, Markets for ideas. Marzo 2010 LSSI and Notice.

- Apartados 3º y 4º: Modifican el Texto Refundido de la Ley de Propiedad Intelectual (en adelante LPI)

- Apartados 5º a 8ª: Modifican la Ley 29/1998 de la Jurisdicción Contencioso-Administrativa. (en adelante LJCA)

Estas modificaciones legales tienen como finalidad reforzar las medidas de protección de la propiedad intelectual en el ámbito de la Sociedad de la Información.

A continuación analizaremos los apartados 1º a 4º:

Apartado 1º:

Se introduce una nueva letra e) en el art. 8.1. LSSI, que regula las restricciones a la prestación de servicios, con el siguiente tenor:

e) La salvaguarda de los derechos de propiedad intelectual.

El Anteproyecto pretende igualar "la salvaguarda de los derechos de propiedad intelectual" al resto de bienes jurídicos protegidos por el Art. 8.1 LSSI. Sin embargo el Informe mantiene que no es lo mismo la producción y creación literaria, que si son derechos fundamentales recogidos en el art. 20.1.b CE, que los derechos de propiedad intelectual regulados en la LPI, que no disponen de dicho carácter constitucional.

Apartado 2º: Introduce un nuevo apartado segundo del art. 8 LSSI

2. Los órganos competentes para la adopción de las medidas a que se refiere el apartado anterior, con el objeto de identificar al responsable del servicio de la sociedad de la información que está realizando la conducta presuntamente vulneradora, podrán requerir a los prestadores de servicios de la sociedad de la

información la comunicación de los datos que permitan tal identificación a fin de que pueda comparecer en el procedimiento. Los prestadores estarán obligados a facilitar los datos de que dispongan[26].

Se hace necesario enlazar este apartado con la modificación introducida en el artículo 158 de la LPI: Comisión de Propiedad Intelectual.

1. Se crea en el Ministerio de Cultura, la Comisión de Propiedad Intelectual, como órgano colegiado de ámbito nacional, para el ejercicio las funciones de mediación y arbitraje y de salvaguarda de los derechos de propiedad intelectual que le atribuye la presente Ley.

La introducción de este apartado segundo del art. 8 LPI está dirigido a identificar al responsable del servicio de la sociedad de la información, es decir, al titular de la web que supuestamente esta vulnerando los derechos de propiedad intelectual. Sin embargo, es muy usual que los datos aportados pueden ser ficticios, por lo que sería necesario que los proveedores de servicios aportaran mas datos que los meramente identificativos del titular registrado, lo cual, según el Informe, entraría en contradicción con lo que recoge la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas, que exige en su artículo 6.1 previa autorización judicial para la cesión de datos tales como los de tráfico y localización sobre personas físicas o jurídicas, y datos relacionados necesarios para identificar al abonado o usuario registrado.

El Informe sugiere que se modifique la Ley 25/2007, en el sentido que de no sea necesaria autorización judicial para la cesión de datos relativos a la identidad de abonados o usuarios de las comunicaciones electrónicas siempre que no estén amparados por el secreto de las comunicaciones del artículo 18.3 CE.

[26] http://es.wikipedia.org/wiki/unique-root-draft.hml.

Para aquellos datos relativos a la identidad de abonados o usuarios de las comunicaciones electrónicas que estén amparados por el derecho a la intimidad del art.18.1 CE se estará a lo establecido jurisprudencialmente, valorando la proporcionalidad de la medida.

Según el Informe, lo que en ningún supuesto puede recabar la Comisión ni puede ser proporcionado por los prestadores de servicios de la sociedad de la información son informaciones referidas a comunicaciones privadas que puedan afectar al derecho fundamental al secreto de las comunicaciones, que requieren ineludiblemente autorización judicial.

Apartado 3º:

El Anteproyecto introduce una Disposición Adicional Quinta en la LPI:

El Ministerio de Cultura, en el ámbito de sus competencias, velará por la salvaguarda de los derechos de propiedad intelectual frente a su vulneración por los responsables de servicios de la sociedad de información en los términos previstos en los artículos 8 y concordantes de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información.

Se refiere a la posibilidad de adoptar medidas restrictivas de interrupción de la prestación del servicio o de retirada de contenidos respecto a la prestación de servicios provenientes de prestadores establecidos en España o en otro Estado de la Unión Europea o del Espacio Económico Europeo. Se trata este del apartado más conflictivo y discutido del Anteproyecto, debido sobre todo a la creación de una Comisión de Propiedad Intelectual, dependiente del Ministerio de Cultura, que llevará a cabo dicha labor[27].

Apartado 4º:

[27] http://es.wikipedia.org/wiki/unique-root-draft.hml.

El Anteproyecto modifica el Apartado 158 LPI y crea la Comisión de Propiedad Intelectual:

1. Se crea en el Ministerio de Cultura, la Comisión de Propiedad Intelectual, como órgano colegiado de ámbito nacional, para el ejercicio las funciones de mediación y arbitraje y de salvaguarda de los derechos de propiedad intelectual que le atribuye la presente Ley.

2. La Comisión actuará por medio de dos Secciones.

La Sección Primera ejercerá las funciones de mediación y arbitraje que le atribuye la presente ley.

La Sección segunda velará por la salvaguarda de los derechos de propiedad intelectual frente a su vulneración por los responsables de los servicios de la sociedad de la información, pudiendo adoptar las medidas para que se interrumpa la prestación de un servicio de la sociedad de la información o para retirar los contenidos que vulneren la propiedad intelectual por parte de un prestador con ánimo de lucro directo o indirecto, o de quien pretenda causar un daños patrimonial.

El Informe pone de manifiesto que el introducir la expresión “de quien pretenda causar un daños patrimonial” puede inducir a confusión al considerar que se amplia a cualquier sujeto, aunque no sea un prestador de servicios o responsable de los mismos, lo cual se contradice con lo establecido en la propia Disposición Final primera al modificar la LSSI y con la Disposición Adicional Quinta de la LPI introducida por la misma. La regulación del procedimiento a través del cual la Comisión ejercerá las funciones atribuidas se difiere a una regulación posterior, lo cual crea una gran inseguridad y desconfianza entre los afectados.

Conclusiones

El Anteproyecto analizado ha creado gran alarma social entre los cibernautas y entre distintas asociaciones y colectivos, ya que consideran que esta normativa va permitir a la Comisión de Propiedad Intelectual restringir o interrumpir Internet a aquellos que permitan el acceso a sitios que atenten contra los derechos de propiedad intelectual recogidos en la LPI, derechos que se equiparan por ende a derechos tales como, por ejemplo, la seguridad pública, la dignidad de la persona en la vertiente de no discriminación por razón de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social.. (…) lo cual no debe ser admisible.

El artículo 20 CE reconoce y protege entre otros, el derecho fundamental a comunicar o recibir libremente información veraz por cualquier medio de comunicación. El ejercicio de dicho derecho solo podrá verse suspendido/limitado mediante autorización judicial, tal y como establece el apartado 5º de dicho artículo: “Solo podrá acordarse el secuestro de publicaciones, grabaciones u otros medios de información en virtud de resolución judicial”.

Los cambios legislativos que afecten a derechos fundamentales han de llevarse a cabo a través de una Ley Orgánica, para cuya aprobación, modificación o derogación exigirá la mayoría absoluta del Congreso, en una votación final sobre el conjunto del proyecto.

Por todo ello, es lógico que se exista un gran debate social, ya que existen opiniones muy enfrentadas, incluso en el mismo Gobierno, como muestra el hecho de que el propio ministro de Justicia, Francisco Caamaño, asegure que el cierre de páginas web que exploten los derechos de autor sin autorización deberá contar siempre con un "control y autorización judicial".

4. LA INFORMACION Y EL DERECHO CONSTITUCIONAL

Dentro del contexto jurídico, la información ha generado implicaciones económicas y sociales importantes, de manera tal que podemos determinar dos aspectos: el derecho constitucional de la información y la información como elemento que hace parte de los derechos de propiedad legítimamente reconocidos. Jurídicamente, el desarrollo de la libertad de expresión tiene sus inicios con el Código de Manu o "Código de las diez libertades humanas esenciales y controles o virtudes necesarias para la vida buena"[28]

Autores como HEGEL[29] considera que para que una cultura pueda desarrollar un pensamiento filosófico es necesario que en el contexto social se tenga la libertad de expresión como la facultad humana que permite el desarrollo del pensamiento.

Con el uso del pergamino y las técnicas de escritura surgieron limitaciones a la libertad de expresión pues estas tecnologías atentaban contra los poderes políticos constituidos. El medioevo occidental tuvo un estancamiento tecnológico pues pocos textos podían ser copiados y pocos tenían acceso a ellos; contraria fue la situación el mundo oriental donde el poder político dominante llevó a la cultura china a inventar elementos industriales como el alto horno aún utilizado en las acerías del mundo, las embarcaciones oceánicas, además de valiosos inventos como el papel y la imprenta, y como lo establece DESANTES[30], con la imprenta el desarrollo de la libertad de expresión implicó un desarrollo de la industria y el comercio.

---

[28] GONZALEZ, Cristóbal, De la libertad de expresión a la libertad de información, Revista Universidad INCCA, abril de 1992. Bogotá, pág 24.
[29] HEGEL, W. Lecciones sobre la historia de la filosofía, Tomo I. México 1977.
[30] Cfr. DESANTES, José María, Fundamentos del derecho de la información, Ed. Confederación Española, Madrid 1977, pág 46.

Los derechos de la clase comerciante fueron confirmados en 1629 con el “Bill of Rigths” y posteriormente en 1679 con el “Habeas Corpus Rigth” convirtiéndola hoy por hoy en la clase dominante, pues se incluyeron libertades que dieron inicios a las declaraciones constitucionales de derechos, razón por la cual en 1789 la libertad de expresión alcanzó su punto máximo al ser establecida en la “Declaración de Derechos del Hombre y del Ciudadano” aprobada en el marco de la revolución francesa, es así como a finales del siglo XIX y comienzos del siglo XX los derechos fundamentales adquieren un gran protagonismo. Es así como en la época de la posguerra con los consecuentes horrores vividos se produjo la proclamación de los derechos humanos: “la declaración de los derechos humanos de 1948”, por lo cual el pontífice Juan XXIII en la encíclica *Mater et Magistra* y la UNESCO hacen un especial reconocimiento de la importancia de la información dentro de la actividad humana, pues ésta se convirtió en el medio más eficaz en el desarrollo del mercado, de la política y de la guerra, creando métodos rápidos, eficaces y seguros de comunicación en caso de confrontación bélica.

En virtud de tal influencia en la sociedad moderna la información y la expresión adquirieron un lugar relevante en los textos constitucionales de los Estados democráticos. La libertad de expresión se convirtió en un derecho reconocido constitucionalmente; así el bien jurídico a proteger era la tecnología de la información.

Textos como el de la Declaración Universal de los Derechos Humanos generaron los desarrollos constitucionales en el mundo a este respecto. Así, en su artículo 19 establece que “todo individuo tiene derecho a la libertad de opinión y expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medo de expresión”. Al decir “buscar,

recibir y difundir información" denota la actitud activa de investigar y expresar y una actividad pasiva que incluye responsabilidades.

En La Declaración Universal de los Derechos del Hombre y del Ciudadano se estableció que "la libre comunicación de los pensamientos y de las opiniones es uno de los derechos más preciados del hombre", y continúa diciendo "todo ciudadano puede, por lo tanto, hablar, escribir e imprimir textos libremente, salvo la responsabilidad que el abuso de esta libertad produzca en los casos determinados por la ley"[31].

Como lo comenta DESANTES "la libertad de expresión es por su misma naturaleza, incapaz de proporcionar al hombre un instrumento jurídicamente hábil para satisfacer su necesidad de información"[32]. Los países miembros de la ONU se comprometieron al cumplimiento de tal cometido a partir de 1962 cuando la organización lo declaró como el año de los derechos humanos, y según sus artículos 55 y 56 los Estados deben hacer lo posible para que dentro de sus regulaciones se implante la cultura de respeto a los derechos humanos (art 55) y que tales derechos deben ser avalados mediante programas para respetar lo dicho en el artículo 55 (art 56). De manera que, la "fuerza vinculante directa" del Derecho Internacional Humanitario solo se consigue con los pactos internacionales.[33].

Así, el 16 de diciembre de 1966 se promulga el *Pacto Internacional de derechos Civiles y Políticos,* suscrito por todos los países miembros de la ONU. En el ámbito americano se gestó el *Pacto de San José de Costa Rica,* nombrado oficialmente como *Convención Americana sobre Derechos Humanos*[34].

[31] Declaración Universal de los Derechos del Hombre. Constitución Política de Colombia. Bogotá. Legis 2000.
[32] DESANTES, J. M., op. Cit.,pág 51
[33] Ibidem. pag 54
[34] Convención Americana sobre Derechos Humanos. Pacto de San José. Artículo 13. Ley 16 de 1972.

4.1. La información y el Derecho Constitucional en Colombia.

Como breve historia recordamos el repudio de las monarquías hacia la expresión libre de las ideas, con hechos como la condena a muerte del comunero Galán, cuando éste buscó la participación del pueblo en las decisiones del Reino español con la llamada "Revolución de los Comuneros" en 1781. Hechos que conllevaron a la traducción de los derechos del hombre hecha por Antonio Nariño y al funcionamiento de la imprenta en 1791, la cual al ser legalmente establecida llevó el nombre de "imprenta patriótica".[35] Dicha publicación tuvo como consecuencia para el prócer la persecución por el reino español, y el consecuente cierre de las imprentas constituidas en Santa Fe de Bogotá.

Luego, en 1809 Camilo Torres redacta el llamado *"memorial de agravios",* en el cual, entre otras cosas, se denuncia la limitación a la libertad de expresión que el monarca español estableció en las Américas. Con la independencia, en 1810, se dan las primeras constituciones provincianas, donde se establece la libertad de prensa o de imprenta como medio para expresar las opiniones. En la Gran Colombia, la Constitución de Cúcuta de 1821 establece por primera vez en una constitución, el derecho a la libertad de expresión. Posteriormente en la Constitución de 1830, se incluye la libertad de expresión y la protección a la intimidad con la inviolabilidad de la correspondencia. Con la Constitución de 1853 se amplía la libertad de expresión a través de la imprenta dándole un carácter absoluto e inviolable, y de manera incoherente, se limita la expresión a través de medios informáticos orales. Más tarde, con la Constitución de 1863 se introduce la libertad de expresión absoluta a todo medio de expresión, sea oral o escrito, asimismo, se consagró que por ningún motivo habría censura.

[35] MARQUEZ ESCOBAR, C. Op Cit.Pág 38.

Sin embargo, en 1886 con la Constitución conservadora de NUÑEZ y CARO, nuevamente se limita el derecho a la libertad de expresión y de prensa, pues en su artículo 42 dice que la prensa "es libre en tiempo de paz; pero responsable con arreglo a las leyes", además estableció el controversial articulo k transitorio, que determinó que "mientras no se expida la ley de imprenta el gobierno queda facultado para prevenir y reprimir los abusos de la prensa", dándole así al ejecutivo, un poder excepcional de represión sobre la expresión impresa.

4.1.1. Constitución de 1991.

Tras acontecimientos como procesos de paz frustrados con grupos armados al margen de la ley, la fracasada guerra contra los carteles de la droga, el inconcebible asesinato del líder Luís Carlos Galán, una reforma constitucional no daba espera. Así, en 1991 se publica nuestra nueva Carta Política, introduciendo nuevas figuras políticas y jurídicas, se incluyeron artículos de tratados internacionales en materia de derechos humanos y en general reformas de todo tipo.

En el artículo 20 de la Carta, se consagró el derecho a la libertad de opinión, expresión y de información, cuyo tenor establece que "[s]e garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la fundar medios masivos de comunicación"[36]. Así en el nuevo texto se fundamentan los derechos a la información, expresión y opinión, los cuales constitucionalistas como Naranjo Mesa, afirma que estas son tres libertades autónomas e independientes que hacen parte de los grupos de las libertades intelectuales, que comparten con la libertad de enseñanza y con la libertad de telecomunicaciones, lo cual se refiere

[36] Gaceta Constitucional Nº 127. pág 3.

a la libertad de fundar medios de comunicación, como variante de la libertad de empresa.

Otras opiniones como la del doctor Mendoza Palomino, encuentra que las libertades de opinión, expresión e información hacen parte de un conjunto de derechos individuales que propenden por la búsqueda de la integridad de la personalidad. Dentro de las libertades, divide las de información y las de expresión por ser interdependientes unas de otras, pero les hace compartir su género por ser libertades, junto a las libertades de enseñanza y las libertades espirituales; todas inscritas aún dentro de las normas protectoras de la personalidad del individuo[37].

El catedrático Mario Madrid-Malo[38], efectúa un sustento filosófico, jurídico y constitucional, al establecer unas libertades llamadas de la comunicación, dentro de las cuales se encuentran las libertades de expresión, difusión e información, sin tener en cuenta la libertad de opinión, pues considera que la libertad de pensamiento no implica necesariamente un acto mental de opinión, y que la libertad de expresión surge como presupuesto para el desarrollo de las libertades de comunicación, ya que sin la opinión éstas no tienen validez; además afirma que antes de la opinión está la autonomía que es la vértebra que sostiene los derechos individuales.

De este modo, la autonomía surge de la libertad de pensamiento de la cual surge la libertad de opinión y de ahí la libertad de información, que se da: como facultad humana para recibir información y como práctica humana para difundir

[37] MENDOZA PALOMINO, Álvaro. Teoría y Sinopsis de la Constitución de 1991. Bogotá, Doctrina y Ley, 1992, pág 245.
[38] MADRID-MALO, Mario. Estudios sobre derechos fundamentales. Bogotá, Tercer Mundo, 1995.

información, para lo cual es necesario tener la libertad de expresión, y para su difusión se da la libertad de fundación de medios masivos de comunicación.[39].

4.1.2. La libertad de información y el Derecho a la Intimidad.

Existen unos derechos fundamentales que se ponen en conflicto con otros derechos fundamentales cuando se dan ciertas situaciones jurídicas de hecho, como es el caso de las libertades informativas o comunicativas confrontadas con los derechos que protegen la intimidad, y con los derechos que protegen la honra, pues con el desarrollo de la industria informativa y la sociedad capitalista se da que los oferentes de servicios buscan dentro del mercado su posible demanda para lo cual recurren a sociedades dedicadas a colectar información de bases de datos de supermercados, tarjetas de crédito, cuentas bancarias, entre otros, para generar un perfil de cada persona, invadiendo así su esfera privada.

Nuestra Carta Magna de 1991 en su artículo 15 estableció el derecho a la intimidad personal y familiar, el derecho al buen nombre, y el derecho a la rectificación de datos, los dos últimos buscan proteger la imagen de cada persona, que por mala información no se dañe *el buen nombre,* sin embargo el derecho a la intimidad se encuentra en pugna con la información y con los derechos de la comunicación.

Para el autor Madrid-Malo, la intimidad es el espacio de la personalidad de los sujetos que no puede llegar a ser por ningún motivo de dominio público, salvo la propia elección, así la intimidad busca proteger el espacio privado, y se estructura como un derecho protector frente al Estado y los particulares en el

[39] MARQUEZ ESCOBAR, C. Op cit. Pág42

campo privado, del cual hacen parte la vida intima, la vida familiar, la vida sexual, las anomalías físicas y síquicas, los secretos sobre el estado civil y la filiación, los escritos privados, la correspondencia de cualquier tipo y las situaciones de angustia, dolor y abatimiento, razón por la cual profesionales como médicos, abogados, sicólogos, sacerdotes no pueden comunicar tal información, convirtiéndose en un derecho protector de la personalidad.

Como lo afirma LYON[40], en la intimidad se encuentra un espacio de doble libertad, libertad de la intrusión del Estado y de la economía, y libertad de revelar lo que se quiere de sí, solo a quien cada cual quiere. Lo privado se desarrolla en contraposición a lo público, por lo cual el derecho a la intimidad o a la privacidad se ha conceptualizado como un derecho fundamental, con el desarrollo de la prensa y de las tecnologías de la información se suele inmiscuirse en la vida de personajes públicos y en reacción a ello se creó la conciencia social de un derecho que protegiera la intimidad y el espacio personal.

4.1.3. La libertad de información y el Derecho al Buen nombre.

Los derechos de carácter público que se pueden ver afectados por las tecnologías de la comunicación son el derecho al buen nombre, como concepto característico de la personalidad, y el derecho a la honra como aspecto psicológico.

La Constitución Política de nuestro país consagra en su artículo 15 el derecho al buen nombre al decir en la primera parte del inciso primero que "[t]odas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar…"[41]

[40] LYON, David. El ojo electrónico. Santafe de Bogotá, Alianza, 1998, pág 253 y ss.
[41] CONSTITUCION POLITICA DE COLOMBIA, Artículo 15. Bogotá, Legis, 1999.

El Pacto Internacional de Derechos Civiles y Políticos, en su artículo 17, al igual que la Convención Americana de Derechos humanos en su artículo 11, numeral segundo, establecen el derecho al buen nombre refiriéndose a éste como la "reputación", la cual no podrá ser objeto de ataque injustificados o ilícitos. Este derecho junto con el de la honra y el honor conforman además del patrimonio moral de la persona, el patrimonio económico pues de él depende el prestigio para el desarrollo de sus actividades económicas.

Según el doctor Mendoza Palomino[42], el derecho al buen nombre pertenece a los derechos que junto a las libertades como las informativas, protegen la integridad de la personalidad, uno de los bienes más preciados del hombre. Este es uno de los bienes jurídicos primarios atribuidos al hombre por su juridicidad natural.

En opinión del doctrinante Madrid-Malo, éste derecho se halla ligado estrechamente con otros derechos como el de la personalidad, el de la igualdad, la intimidad, el *habeas data* y el derecho al desarrollo de la libre personalidad[43].

El derecho al buen nombre, como derecho fundamental debe ser protegido por el Estado proveyéndolo de herramientas frente al poder de la información a fin de proteger su perfil o su imagen, siempre y cuando la persona no se encuentre ante alguna causal que genere tal descrédito público, pues en caso contrario, ante un hecho punible, la persona no puede exigir al Estado la no divulgación de una información que puede afectar la pueblo.

[42] MENDOZA PALOMINO, Álvaro. Teoría y Sinopsis de la Constitución de 1991. Santafé de Bogotá, Doctrina y Ley, 1992, pág 245 y ss.
[43] MADRID-MALO, Op cit., pág 122.

4.1.4. La libertad de información y el Derecho a la Honra.

El derecho a la honra, como derecho público, está consagrado en los artículos 1 y 21 de la Constitución, en el artículo 12 de la Declaración de los Derechos Humanos y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, instituyéndose así la protección del Estado sobre la honra de las personas a través de la ley.

Según el exmagistrado de la Corte Constitucional doctor Naranjo Mesa, "la honra es el sentimiento o la conciencia de la propia dignidad y es también el atributo más valioso que pueda tener la persona frente a los demás", así la protección de la honra es directamente una protección de la dignidad del individuo, además ésta se encuentra tipificada en la legislación penal como delitos de calumnia y difamación.

Al respecto, el doctor SORIA[44] establece que la honra es una emanación de la dignidad humana; el honor como impresión interna de la honra, es uno de los derechos fundamentales de carácter personal y, junto a la vida y la libertad constituyen los valores más preciados del hombre. Dice el autor que, la honra como parte del patrimonio moral representa el primer nivel del honor, y el honor es una proyección de la virtud, de manera que el primer nivel lo constituye el crédito moral o sea, la manera en que se rinde frente a los demás, y el segundo nivel tiene un plano estrictamente valorativo del individuo frente a sí mismo; por esto sus implicaciones en materia de responsabilidad por el llamado *daño moral subjetivo.* De manera tal que la protección jurídica de la honra se refleja en una protección jurídica indirecta del honor, pues la protección de la honra adquiere

[44] Cfr. SORIA, Carlos. Derecho a la honra y derecho a la información. Barcelona, ATE, 1981.

encarnación social y trascendencia en el honor[45]. El derecho a la honra, como derecho "público" no debe depender de categorías subjetivas como el honor, dificultando la labor judicial, pues buscar la *objetividad* de un concepto moderno como la honra, referida a la opinión que tienen los demás sobre sus virtudes, conllevaría a buscar una reforma del concepto moderno de *yo.*

4.1.5. El habeas data.

El habeas data fue establecido como medio legal coercitivo para permitirle a toda persona conocer la información que se tiene de sí en bases de datos, si dicha información es cierta o atenta contra la *data imagen,* a fin de que se rectifique o se elimine si se considera que tal dato vulnera el derecho a la intimidad. La rectificación es necesaria cuando el dato atenta contra la honra y el buen nombre, y la eliminación cuando el dato atenta contra la intimidad o privacidad. Intimidad es el control que nosotros tenemos sobre la información que nos incumbe.

El derecho a la intimidad es reconocido e incluido en las principales declaraciones internacionales de Derechos Humanos. En la Declaración Universal de los Derechos Humanos, artículo 12: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación.

Pacto Internacional de Derechos Civiles y Políticos[46], artículo 14.1: La prensa y el público podrán ser excluidos de la totalidad o parte de los juicios cuando lo

[45] MARQUEZ ESCOBAR, Op cit, pág 59.
[46] Pacto Internacional de Derechos Civiles y Políticos. Artículo 14 de la Ley 74 de 1968.

exija el interés de la vida privada de las partes. Artículo 17.1 del mismo Pacto: Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honor y reputación.

Convenio para la protección de los Derechos humanos y las libertades fundamentales. Roma 4 de noviembre de 1950, artículo 8.1: Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. Declaración Americana de Derechos Humanos, artículo 9: Toda persona tiene derecho a la inviolabilidad de su domicilio. Artículo 10: Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia.

Pacto de San José de Costa Rica[47], artículo 11.2: Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Artículo 11.3: Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Declaración de los Derechos y Libertades Fundamentales. Parlamento Europeo, mayo 16 de 1989, artículo 6.2: Se garantizará el respeto de la esfera privada y de la vida familiar, del honor, del domicilio y de las comunicaciones privadas. Artículo 11.2: No podrá obligarse a nadie, en su vida privada, a revelar su pertenencia a una asociación, a no ser que esta sea ilegal.

Carta Africana de los Derechos del Hombre y de los Pueblos. 1981, artículo 4: La vida humana es inviolable. Todo ser humano tiene derecho al respeto de la vida

[47] Convención Americana sobre Derechos Humanos. Pacto de San José. Artículo 11. Ley 16 de 1972.

y la integridad física y moral de su persona. Nadie puede ser privado arbitrariamente de este derecho.

La Constitución de 1978 en España, artículo 18: Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en casos de flagrante delito. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Constitución de Paraguay de 1992: La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la ley o a los derechos de terceros, está exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas.

Colombia no tiene mayor desarrollo legislativo del *habeas data.* La Constitución Política de 1991, artículo 15: el derecho a la intimidad personal y familiar, el derecho al buen nombre, el habeas data y el respeto a la libertad y demás garantías consagradas en la Constitución, en la recolección, tratamiento y circulación de datos. Artículo 20: Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación.

El artículo 58 es tomado como base constitucional tratándose de conflictos de derechos: Cuando de la aplicación de una ley expedida por motivo de utilidad pública o interés social, resultaren en conflicto los derechos de los particulares con la necesidad por ella reconocida, el interés privado deberá ceder al interés público o social, y el carácter de interés público del artículo 335: las actividades financiera, bursátil, aseguradora y cualquier otra relacionada con el manejo, aprovechamiento e inversión de los recursos de captación a las que se refiere el literal d) del numeral 19 del articulo 150 son de interés público…[48].

En palabras del constituyente Uribe Vargas:

> "El principio del habeas data, abarca no solo la garantía del buen nombre, sino el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido acerca de la propia persona en bancos de datos y en archivos de entidades públicas y privadas.
>
> "El riesgo que tiene para las personas el que las viejas y erradas informaciones sigan gravitando sobre su buen nombre, se ha convertido en una de las modalidades de más peligro para la intimidad de las personas y para el desarrollo de su personalidad"[49].

El habeas data es una herramienta apta para conocer la violación, tanto en lo privado –cuando se viola la intimidad- como en lo público, cuando se viola el buen nombre o la honra, sin embargo no lo es para eliminar la trasgresión y resarcir los daños ocasionados por la violación ya que necesita de distintos mecanismos jurídicos de responsabilidad constitucional, civil y penal, como es el

[48] CONSTITUCION POLITICA DE COLOMBIA. Ministerio de Justicia y del Derecho. Bogotá,1996.
[49] Gaceta Constitucional Nº 82, pág 12.Citado por LLeras de la Fuente, Carlos, Tangarife Torres, Marcel. Constitución Política de Colombia. Origen, evolución y vigencia. Bogotá, Diké, 1996.

caso de la acción de tutela, la cual se instituyó en nuestra Carta como mecanismo constitucional para eliminar las violaciones tanto públicas como privadas de los derechos fundamentales, además está el mecanismo de rectificación de datos el cual se encuentra constitucional y legalmente reglamentado, por el cual el medio masivo de comunicación que suministró la información debe rectificar en las mismas condiciones dicha información errónea[50].

El habeas data se manifiesta en tres facultades que tiene toda persona: el derecho a conocer las informaciones referidas a ella, el derecho a actualizar esas informaciones agregándoles los nuevos datos y el derecho a rectificar las informaciones que no corresponden a la verdad. El núcleo esencial del *habeas data* lo integran la autodeterminación y la libertad económica que puede verse afectada por la circulación de datos no veraces o no autorizados por la ley o por su titular. De este núcleo se deduce el Derecho a la caducidad del dato negativo.

[50] Ley de rectificación, artículo 20.

5. LA INFORMACION COMO BIEN POLITICO, ECONOMICO Y JURIDICO.

Desde el punto de vista político, el acceso a la información es un derecho fundamental que solo puede ser limitado por conveniencia para el desarrollo del Estado, desde lo económico y jurídico, la información es un bien que económicamente permite ser transado a través del mercado, convirtiéndose tanto en factor de producción como en producto, además es considerado jurídicamente como objeto de la propiedad, pues como bien económico es objeto del poder, lo cual conlleva a que el derecho genere un sistema de protección a dicho bien económico.

Así, la propiedad como tal es un instrumento de dominio económico y desde lo jurídico es un mecanismo de protección, el cual encuentra sustento en el artículo 58 de nuestra Constitución, éste garantiza a toda persona el libre acceso a la propiedad y el respeto por la propiedad privada. En el inciso segundo dispone que la propiedad es una función social que implica obligaciones, es decir que ante conflictos prima el interés general haciendo posible ejercer la expropiación[51].

El sistema de protección al aspecto económico de la propiedad, en cuanto al derecho privado se encuentra reglamentado en el artículo 669 de nuestro Código Civil donde lo clasifica como un "derecho real en una cosa *corporal,* para gozar y disponer de ella arbitrariamente, y no siendo contra la ley o derecho ajeno. *Corporales* es decir que "tienen un ser real y pueden ser percibidas por los sentidos".

[51] Con el acto legislativo número 2 de 1999, la expropiación se redujo a una institución simbólica cuya cabida es excepcional.

Un bien es considerado jurídicamente como tal debido a su posibilidad de apropiación y desde el punto de vista económico a su cuantificación. Según el postulado de CARNELUTTI la propiedad de las cosas nace en la economía antes que el mismo derecho[52].

La doctrina económica distingue los bienes públicos de los bienes privados: un bien público es aquel que es *no excluible* y *no rival,* esto quiere decir que su consumo por parte de un individuo *no* reduce la cantidad de que puedan disponer los demás y, *no* es posible excluir de su consumo por lo menos a una persona, es el caso de las carreteras, el mar, el alumbrado público entre otros.

Desde este punto de vista, la información la podemos clasificar como un bien *no rival* y *no excluyente*, de manera que es en principio un bien público, pero ante todo es un derecho fundamental. Es bien público debido a la ausencia de restricciones de acceso y exclusión, sin embargo es bien privado intermedio debido a la existencia de mecanismos constitucionales, legales y de mercado que determinan si se permite o no la exclusión de consumidores de información.

Entonces, ya se determinó que la información jurídicamente es un bien, pero qué tipo de bien?, pues la legislación establece que algo por el hecho de ser bien adquiere el carácter de cosa, no obstante las cosas pueden ser corporales como también incorporales. Y según la legislación civil, son bienes corporales los muebles e inmuebles, siendo muebles los que por su naturaleza se pueden trasladar de un lugar a otro, los inmuebles no se pueden trasladar sin afectar su naturaleza, y los incorporales son solo, derechos. Esta definición del bien información afecta la concepción jurídica ya que no se ajusta dentro de la definición de bien incorporal hecha por la legislación, en conclusión no hay una

[52] CARNELUTTI, Franccesco. Cómo nace el derecho. Bogotá, Temis, 2000. Pág 33.

categoría donde pueda ubicarse la información como bien. Sin embargo, la información es un bien jurídicamente protegido a través del derecho de propiedad.

El Código Civil en su artículo 671 establece que toda producción del talento y el ingenio es propiedad de su autor, de manera que la propiedad que reconoce el derecho civil de la propiedad intelectual recae sobre la información; dado que sobre los bienes se reconoce el derecho de propiedad, la existencia del reconocimiento de propiedad sobre la información es necesariamente un reconocimiento del carácter de bien que tiene la información. De manera tal que la legislación colombiana reconoce el derecho de propiedad de la información y, causalmente, reconoce la existencia de la información como bien[53].

Entonces, la información como bien, económicamente es no-rival y puede ser excluyente o no excluyente, lo cual determina algunos elementos de carácter jurídico, pues la doctrina determina como elementos del derecho de propiedad la capacidad de uso, fruto y disposición; el que un bien sea no-rival implica que su consumo por parte de un individuo *no* reduce la cantidad del bien que pueden disponer los demás. Así, como los bienes informáticos son no-rivales, toda persona tiene capacidad de uso e incluso de disfrute pero no el derecho de disposición, pues la información al ser económicamente considerada como un bien público aplica disposiciones constitucionales o legales que no permiten excluir dichos bienes los cuales demanda todo tipo de consumidores. Y es considerada económicamente como bien privado cuando los mecanismos de exclusión constitucionales o legales de mercado son asignados a demandantes exclusivos.

[53] CODIGO CIVIL. Compilado por ORTEGA, Jorge. Bogotá, Temis, 1969. Artículo 671

Hay cierta información que como bien tiene un carácter público, sobre la cual el derecho reconoce la capacidad de cada persona de obtenerla y expresarla, como es el nombre, el estado civil, número telefónico, dirección de residencia e incluso su misma imagen, sin embargo cualquier persona puede recolectar esta información, crear una base de datos y lucrarse de ella. Este es un bien informático que es protegido por el Estado siempre y cuando la información contenida se ajuste a la realidad y el único que puede disponer de ella es su titular, para lo cual el derecho constitucional le concede el ya mencionado derecho del *habeas data.*

En nuestro país la ley 527 de 1999, en su artículo 10 reconoció fuerza probatoria a los mensajes de datos:

> *"Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del capítulo VIII del título XIII, sección tercera, libro segundo del Código de Procedimiento Civil.*
>
> *En toda actuación administrativa o judicial no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el solo hecho de que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original".*

El artículo 14 de la misma ley establece que *"…No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos…"*

El artículo 2 define el mensaje de datos como la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares,

como el intercambio electrónico de datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax.

Dicha ley en el parágrafo del artículo 28 atribuye automáticamente los mismos efectos de una firma autógrafa a la firma digital que reúna los siguientes requisitos: a) Es única la persona que la usa; b) es susceptible de ser verificada; c) está bajo el control exclusivo de la persona que la usa; d) está ligada a la información o mensaje de manera que si son cambiados la firma digital es invalidada; y e) está conforme a las reglamentaciones adoptadas por el gobierno nacional[54].

En una sociedad de gran diversidad, los medios de comunicación desempeñan un papel relevante en la tarea de unificar la información sin dar importancia desde que punto social o geográfico se geste. Al igual que el conjunto de las relaciones sociales, la información se ve afectada por las diferentes transformaciones que vive la sociedad, por tanto es influenciada por conflictos de interés, por la arrolladora lógica del capitalismo y por la indefinida lista de conflictos que se presentan en el mundo. El hecho de que un sujeto cualquiera reciba señales informativas de lo que ocurre a su alrededor y que lo afecten directa o indirectamente, es conducente a la toma de decisiones ya sean de carácter individual o colectivo.

[54] LEON MONCALEANO, William Fernando. De la Comunicación a la Informática Jurídica Penal Bancaria.Ed. Doctrina y Ley Ltda.. Bogotá 2001. Pág 97.

6. MARCO LEGAL SOBRE LA INFORMÁTICA.

A partir de la década de los setenta, surgió una relación entre informática y telecomunicaciones con un flujo de datos transnacionales o fronterizos, de ahí el nuevo concepto de teleinformática o telemática. El intercambio internacional de la información, representa un valor económico que se percibe a través de las multinacionales de crédito, o en efectivo cuando se cobran los servicios en el país de origen, porcentajes relevantes en la actual economía mundial. Este flujo de datos se inició en el siglo XX con el avanzado desarrollo de las comunicaciones, de los sistemas inalámbricos, de la utilización de satélites, lo cual hizo necesaria la creación de gran normatividad encaminada a la regulación de las telecomunicaciones en el mundo.

"El **Convenio Internacional de Comunicaciones de Montreaux de 1965**, es considerado la culminación de un dilatado proceso de formación jurídica, éste define la comunicación como: "Toda transmisión, emisión, o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de toda índole mediante hilo, radioelectricidad, por un procedimiento óptico u otros de carácter electromagnético". Adicionalmente, establece el principio de que todos los Estados deben tolerar el tránsito de telecomunicaciones. Así, la información es un fenómeno mundial que debe estar al alcance de todos y que puede transitar libremente de Estado a Estado, reiterando el principio de la libertad de información e informática, acorde a los progresos técnicos de la sociedad.

A nivel de disposiciones normativas, en Colombia pueden citarse los estatutos de los medios masivos de comunicación (radio y televisión, los cuales por intereses políticos no se han decantado y son continuamente reformados).

Igualmente **la Ley 72 de 1989**, que definió los nuevos conceptos y principios sobre la organización de las telecomunicaciones en nuestro país y sobre el régimen de concesiones de los servicios.

El Decreto 131 de 1976 dictó normas sobre la utilización de sistemas de comunicación y de equipos y servicios de procesamiento de datos, el cual fue reglamentado por el Decreto 260 de 1988, referente a la contratación de servicios informáticos, los cuales se contratarán conforme a las normas y procedimientos que para cada caso en particular señala el Estatuto de Contratación.

La Constitución Política de 1991 en su artículo 15, establece el derecho que toda persona tiene a su intimidad personal, familiar y a su buen nombre; allí mismo expresa la inviolabilidad de la comunicación privada. De otra parte el derecho constitucional al *habeas data,* encuentra su impulso y desarrollo jurisprudencial en el surgimiento del poder informático[55] y la posibilidad del manejo indiscriminado de los "datos personales". La Corte Constitucional teniendo en cuenta los artículos 15 y 16 de nuestra Carta, le ha reconocido existencia y validez ha llamado derecho a la autodeterminación informática[56]. Así, ante la revisión a las sentencias SU-082 1995, T-552 1997, T-729 2002 entre otras, la intimidad no es otra cosa que el derecho de una persona de semejar su propia existencia como a bien lo tenga con el mínimo de injerencias exteriores; por su naturaleza individualista y negativa concepciones como estas hoy son insuficientes para demandar la protección del ordenamiento ante las

[55] En sentencia T-414 de 1992, la Corte Constitucional, definió poder informático como una especie de "dominio social sobre un individuo", consistente en "la posibilidad de acumular informaciones en cantidad ilimitada, de confrontarlas y agregarlas entre sí, de hacerles seguimiento en una memoria indefectible, de objetivizarlas y trasmitirlas como mercancías en forma de cintas, rollos o discos magnéticos".

[56] Derecho innominado a "conocer, actualizar y rectificar las informaciones recogidas en archivos y bancos de datos" de que trata el arículo 15 de la Constitución, asociado al concepto de *habeas data,* la Corte en sentencia SU-082 de 1995 lo definió cono derecho a la "Libertad informática".

nuevas tecnologías de punta, concretamente en el sistema informático electrónico.

El **Decreto 663 de 1993**, por medio del cual se actualiza el Estatuto Orgánico del Sistema Financiero y se modifica su titulación y numeración, establece en su artículo 127 Nº 6 "Libreta. Con excepción de lo dispuesto en el artículo 126 numeral 2, ningún establecimiento bancario podrá pagar depósitos de ahorros, o una parte de ellos, o los intereses, sin que se presente la libreta u otra constancia de depósito y se haga en ella el respectivo siento al tiempo de pago, salvo en aquellos casos en que el pago se produzca mediante la *utilización por parte del usuario de un medio electrónico que permita dejar evidencia fidedigna de la transacción realizada".* Y el artículo 139 –Cobro de los Servicios Ofrecidos a los Depositantes. Las corporaciones de ahorro y vivienda podrán cobrar por todos los servicios que presten a sus depositantes, tales como suministros de libretas de cuentas de ahorro, transferencias de fondos y uso de los sistemas electrónicos de depósito y retiro.

La **ley 222 de 1995,** por la cual se modifica el Libro II del Código de Comercio, se expide un nuevo régimen de procesos concúrsales y se dictan otras disposiciones, en su artículo 19. REUNIONES NO PRESENCIALES. Siempre que ello se pueda probar. Habrá reunión de la junta de socios, de asamblea general de accionistas o de junta directiva cuando por cualquier medio todos los socios o miembros puedan deliberar y decidir por comunicación simultánea o sucesiva.

La **Ley 223 de 1995, Decreto Reglamentario Nº 1094 de 1996,** hace referencia a la emisión de facturas electrónicas, la generación de ahorro para la empresa y el mayor control en la fiscalización, como el caso de los servicios públicos, donde las empresas prestadoras hacen llegar a sus usuarios una factura electrónica, la

cual igualmente puede ser cancelada vía telefónica, utilizando la red mundial de Datos “Internet”.

Esta herramienta va dirigida principalmente a grandes consorcios que requieren esquemas de facturación simplificada en grandes volúmenes, igualmente es solución a pequeñas y medianas empresas y en general a usuarios con compromisos adquiridos en virtud de negociaciones y transacciones comerciales. La factura electrónica es un documento legible, que puede ser presentado ante las entidades públicas y los Tribunales. Admite almacenamiento e inalterabilidad en el tiempo, facilita la revisión y posterior auditoria para fines contables, además puede ser reglamentaria como el caso de la factura electrónica de la DIAN.

El **Decreto 1487 de 1999,** “Por medio del cual se autoriza el Sistema Declaración y Pago Electrónico de la DIAN y se establecen algunos parámetros operativos para la presentación de las declaraciones tributarias y el pago de los impuestos por vía electrónica”. Y la **Resolución 0831 de 1999** “Por la cual se adopta y establecen los parámetros operativos del Sistema Declaración y Pago Electrónico de la DIAN, para presentar las declaraciones tributarias y efectuar los pagos de los impuestos administrados por la Dirección de Impuestos y Aduanas Nacionales y de las retenciones en la fuente”. De igual forma se acepta y ratifica la utilización del RUT, para el contribuyente registrado en el Sistema de Declaración y Pago Electrónico.

Este sistema de pago pretende evitar la evasión, demora y agilizar el pronto pago tributario, proporcionando estabilidad y agilización al sistema de recaudo lo cual ha sido siempre una preocupación para el Estado.

La **Ley Modelo de Comercio Electrónico de 1996, de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional CNUDMI,** sirvió de texto guía para la elaboración de la ley 527 de 1999.

"Esta ley modelo se basa entre otros, en el principio del equivalente funcional, el cual consiste en determinar si las funciones de un requisito de forma consignado sobre el papel, se puede cumplir con técnicas o métodos asociados con el denominado comercio electrónico"[57]

El principio de equivalencia funcional del método de firma electrónica, cumple con las funciones que se le atribuyen a una firma manuscrita en las comunicaciones consignada sobre el papel. Esta ley modelo facilita el empleo de las técnicas de comunicación modernas en todas las actividades, con un conjunto de reglas internacionales aceptadas que imprimen certeza jurídica a los actos efectuados a través del uso de la tecnología.

La **Ley 527 de 1999** aprobada por el Congreso, sobre: "Comercio electrónico y firmas digitales" se encuentra encaminada a establecer que los actos de comercio de que trata el artículo 20 del C. C. son objeto de comercio electrónico, que contiene disposiciones relativas a la oferta mercantil vía electrónica que complementa las disposiciones del artículo 845 y ss. del C. C.; y complementa la normatividad mercantil de los contratos de transporte de mercancía que requieren de documentación (informaciones) que pueden ser transmitidas vía electrónica y la ley señala los requisitos de su emisión.

Curiosamente esta Ley cuya finalidad es la de dotar de validez legal a la información electrónica, es poco aplicada en ámbitos privados y públicos, los

[57] MAGISTRADO PONENTE Dr MORON DIAZ, Fabio. Corte Constitucional. Comisión de Naciones Unidas para el desarrollo del Derecho Mercantil Internacional- UNCINTRAL- Sentencia 662 de 2000.

cuales invierten cada vez más recursos en tecnologías de información y comunicación con el fin de apoyar la gestión. Sin embargo, dicha ley que reposa silenciosa en los Códigos y que no se pone en práctica, comprende una normatividad proactiva para asegurar y proteger jurídicamente la información digital.

Pero, por qué no tiene mayor aplicación en Colombia, la Ley 527 de 1999, en las empresas y en el Estado. En las compañías no se aplica en forma eficaz, simplemente porque no la conocen o no ven como un riesgo potencial el hecho de que su información no sea reconocida como válida o con mérito probatorio en instancias administrativas o judiciales. De otro lado, son escasas las sentencias o providencias referidas a la validez o alcance probatorio de la información electrónica o de los mensajes de datos en casos particulares y que desarrollen los principios y reglas de la Ley 527.

En el Estado, no tiene mayor aplicación la Ley 527, entre otras, por las siguientes razones:

Porque no se ha adoptado un “reglamento” que establezca las reglas de validez de los mensajes de datos y las firmas electrónicas que se utilizan al interior de la administración pública.

Porque en diferentes niveles del Estado, se siguen adelantando discusiones de nunca acabar sobre el modelo de certificación digital más conveniente para el sector público.

Porque el Decreto 1747 de 2000, que reglamentó la Ley 527, estableció restricciones legales para el uso de certificados electrónicos en ambientes

cerrados. Este decreto está en mora de ser revisado y ajustado a las realidades del mundo tecnológico y a la dinámica de los negocios electrónicos.

Porque nuestros jueces y servidores públicos después de cinco años de vigencia de la ley y a casi diez del comienzo de la masificación de Internet, siguen sitiados por la cultura del papel y de las firmas manuscritas.

En auto 2475 de noviembre de 2003, de la Superintendencia de Industria y Comercio, esta entidad expresó que: "es importante anotar que los correos electrónicos anexados a la demanda no pueden ser tenidos como prueba en este estado del proceso, porque se trata de documentos privados, no auténticos, pues no existe certeza acerca de quién los elaboró, toda vez que no están manuscritos ni firmados". La Superintendencia cuando emitió este auto realizó una interpretación restrictiva del artículo 7 de la Ley 527 de 1999, que no define la firma electrónica en los términos y con las características de una firma manuscrita.

En la actualidad, jueces de otros países que aplican principios legales, similares a los definidos en nuestra ley, aceptan que los correos electrónicos, pueden ser admitidos judicialmente como documentos auténticos, en la medida en que la intención de las partes así lo exprese. Este es el caso de una decisión de la Corte de Apelación del Reino Unido, que señaló que la conclusión de un contrato, no se relaciona exclusivamente con el uso de una firma (manualmente escrita o electrónica), sino que debe depender primariamente de la intención de las partes[58]

En otras causas, algunos jueces han concluido que los *e-mails* pueden entenderse como documentos firmados. Es el caso de un Juez griego que aceptó que un

[58] Caso Pretty Pictures Sarl vs. Quixote Films Ltda (2003) EWHC 311 (QB).

correo electrónico, puede satisfacer las funciones legales de una firma (única identificación del firmante, como único vínculo entre el firmante y su dirección de correo electrónico). Y, por lo tanto, puede ser considerado como el equivalente electrónico de una firma manual[59].

El **Decreto 2170 de 2002** "Por el cual se reglamenta la ley 80 de 1993 se modifica el decreto 855 de 1994 y se dictan otras disposiciones en aplicación a la ley 527 de 1999". Con este decreto, el Estado colombiano, busca la modernización, es así como establece la ejecución de un proceso de contratación pública a través de la red, desde la publicación de los pliegos hasta la adjudicación.

La **Ley 794 de 2003,** reforma el Código de Procedimiento Civil, e impone en su artículo 29 la obligación de registrar una dirección electrónica en el registro mercantil para recibir notificaciones judiciales. La obligatoriedad es obvia, la norma no dice "podrán registrar" sino "deberán registrar una dirección electrónica", lo cual es inaceptable para un comerciante que no tiene actividad en línea, que deberá revisar su correo con cierta frecuencia para que no sea desactivado.

Cabe anotar que, aunque es meritorio el interés del legislador colombiano de estar a tono con la nueva Sociedad de la información, al introducir los medios tecnológicos en el ámbito de la administración de justicia, se considera un desacierto la exigencia legal del correo electrónico tal y como está planteada.

[59] Decisión 1327 de 2001 de la Corte de Primera Instancia de Atenas

7. EL DOCUMENTO ELECTRONICO.

Según el doctrinante nacional Devis Echandía, el documento es: "toda cosa que sirve de prueba histórica indirecta y representativa de un hecho cualquiera". Por su parte, el tratadista internacional Carnelutti, considera que "el documento no es sólo una cosa, sino una cosa representativa, o sea capaz de representar un hecho".[60]

Con respecto a la naturaleza jurídica del documento electrónico, Eugenio Gaete señala: "Preferimos situar la naturaleza jurídica propia del documento informático en una nueva forma, surgida al amparo de las modernas técnicas de electrónica, como un elemento vital para el desarrollo de un nuevo concepto de comercio y por ende de los contratos a través de los cuales éste se expresa hoy y se expresará cada vez más en el futuro cercano. No tenemos duda de que toda la teoría de los contratos es perfectamente asimilable a la nueva forma instrumental, lo es incluso la teoría de la prueba, la cual sea que considere al informático, como un instrumento privado o público, deberá necesariamente modernizarse y adaptarse a la consideración valórica que éste debe llegar a tener en el concierto de los medios probatorios".

"Todo ello requiere de reformas legales y la dictaminación de normas nuevas destinadas a producir su adaptación en un mundo normativo que evidentemente, al día de hoy, privilegia sutantivamente al documento tradicional".

"Se requiere de una visión legislativa destinada a proveer a los Estados de leyes necesarias para dar el gran paso adelante, y si ello no ocurre, por simple

[60] GAETE GONZÁLEZ, Eugenio, Instrumento público electrónico, Barcelona, Bosch, 2000, p. 188.

necesidad adaptativa -toda vez que el derecho no puede quedar tras la realidad social circundante- será preciso recurrir a la vía interpretativa".

El documento electrónico se define como "La representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser representados en una forma humanamente comprensible"[61].

Así, el documento electrónico, es un bien de naturaleza mueble, que puede ser trasladado de un lugar a otro y puesto a consideración del juez. Y se caracteriza por lo siguiente:

- Se trata de un bien mueble representativo de un hecho o de un acto del hombre.
- Esa representación se da por medio de signos inteligibles.
- Es susceptible de llevarse o transportarse al proceso.

De manera tal que el mensaje de datos, entendido como documento electrónico, es susceptible de ser firmado, de tener un titular o creador, e, igualmente, puede diferenciarse cuando un mensaje de datos es un documento electrónico original y auténtico, en la medida en que no ha sido alterado. Así mismo, se podrá deducir que son aplicables las distinciones entre documento electrónico público y privado en los mismos términos que trae la ley procesal civil colombiana[62].

[61] Proyecto Ediforum, citado en Santos, Jaime Eduardo et al., Proyecto académico para penalizar la criminalidad informática, Bogotá, s. e., noviembre, 1997, p. 9.

[62] Esta noción resulta de interés en la medida que tanto los particulares como el Estado se manifiesten por medios de divulgación electrónica. Así, por ejemplo, un correo electrónico prove niente de un funcionario público en ejercicio de sus funciones será documento público por ese sólo hecho. Así mismo, resulta indicativo de la connotación de documento público, la documentación electrónica que se contenga en las direcciones electrónicas cuyo nombre de dominio termine en punto gov (.gov}, puesto que éstas son exclusivas de los entes estatales, siendo su usurpación una forma de falsedad en documento público.

El artículo segundo de la ley 527 de 1999, define el mensaje de datos en los siguientes términos: "Mensaje de datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax".

La honorable Corte Constitucional se refirió al contenido del mensaje de datos, en el siguiente sentido:[63]

> La noción de *mensaje* comprende la información obtenida por medios análogos en el ámbito de las técnicas de comunicación modernas, bajo la configuración de los progresos técnicos que tengan contenido jurídico. [...]
>
> Cuando en la definición de mensaje de datos se mencionan los "medios similares", se busca establecer el hecho de que la norma no está exclusivamente destinada a conducir las prácticas modernas de comunicación sino que pretende ser útil para involucrar todos los adelantos tecnológicos que se generen en un futuro.

Por consiguiente, el mensaje de datos debe recibir el mismo tratamiento que los documentos consignados en papel, es decir, debe dársele la misma eficacia jurídica, por cuanto el mensaje de datos comporta los mismos criterios de un documento.

Desde este punto de vista, el mensaje de datos, es una prueba de la existencia y naturaleza de la voluntad de las partes de comprometerse; es un documento legible que puede ser presentado ante las entidades públicas y los tribunales; admite su almacenamiento e inalterabilidad en el tiempo; facilita la revisión y posterior auditoría para los fines contables, impositivos y reglamentarios; afirma derechos y obligaciones jurídicas entre los intervinientes y

[63] Sentencia del 8 de junio de 2000, con ponencia de Fabio Morón Díaz.

es accesible para su consulta, así, la información en forma de datos computarizados es susceptible de leerse e interpretarse.

De lo anterior se infiere la importancia del mensaje de datos, pues éste es el soporte electrónico con base en el cual se sustentan y se prueban las relaciones que se establezcan en los entornos electrónicos.

Sin embargo, los documentos que instrumentalizan los mensajes de datos para su emisión presentan algunos inconvenientes respecto a los documentos tradicionales en papel:

- El contenido de un documento electrónico está consignado sobre un soporte electrónico (magnético, óptico...) no apreciable por los sentidos. Su contenido está representado por signos, códigos binarios, que deben ser descodificados mediante un programa, con un procedimiento lógico que convierta la expresión en codificación informática a lenguaje natural.

- Lo obsoleto de las tecnologías que intervienen en la generación y el almacenamiento de estos documentos, equipos y aplicaciones, y la fragilidad de los soportes en los que se conservan. Lo idóneo sería un soporte estandarizado universal.[64]

- La mutación de la información electrónica. Esto queda de manifiesto en la reutilización de soportes, al destruir la información almacenada y la sustitución automática de datos en documentos dinámicos.

- Virtualidad de la información apreciable, sobre todo en los documentos telemáticos,[65] como en el correo electrónico, que es eliminado sin control, privando a los organismos de parte de sus documentos de comunicación.

[64] En el último DLM-Forum celebrado el 18 y 19 de octubre de 1999 en Bruselas, se realiza un llamamiento a la industria informática pidiéndole que se involucre en la elaboración de un modelo de gestión de los documentos y archivos electrónicos, el cual tenga en cuenta los criterios especificados para los archivos y las administraciones públicas, y la adopción de estándares. Este documento se encuentra disponible en htpp://www.dlmforum.eu.org.

- Ubicuidad de la información que es usada por varios organismos que la comparten, lo que impide, en muchos casos, identificar al productor[66].

- Dificultades para identificar el tipo y la forma documental de estos documentos. La forma documental (original, copia...) tiene especial relación con el valor probatorio de estos documentos, o, lo que es lo mismo, con su validez jurídica.

7.1. El documento electrónico y su valor probatorio

Una vez fijados los presupuestos sobre el documento electrónico, se señalan, los antecedentes que la normatividad colombiana ha establecido al respecto, siguiendo parte del trabajo realizado por el profesor Ernesto Rengifo García, en la Universidad Externado de Colombia:[67]

1. El artículo 175 del Código de Procedimiento Civil dice: "Medios de prueba: sirven como pruebas la declaración de parte, el testimonio de terceros, el dictamen pericial, la inspección judicial, los documentos, los indicios y cualesquiera otros medios que sean útiles para la formación del convencimiento del juez". O sea que de las teorías acerca del número y clase de medios de prueba (la legalista, la doctrina analógica y la referencial), fue acogida por

---

[65] El término documento telemático, está empleado en el real decreto 263/1996 de 16 de febrero, por el cual se regula el uso de técnicas electrónicas, informáticas y telemáticas por la administración general del Estado. Davara, M. A., Validez y eficacia jurídica de los documentos generados por medios informáticos o telemáticos: la autenticación de intervinientes y contenidos, s. L, Ligall, 1999, pp. 13-37, no comparte estas denominaciones utilizadas por el real decreto. Zapatero Lourinho, A. S., "El documento telemático: concepto, naturaleza y validación", en Actas de las X
Al respecto se puede ver a López Alonso, Rosa, El documento electrónico en Europa, Facultad de Traducción y Documentación, Universidad de Salamanca.
Jomadas de Archivos Municipales [El Escorial, 2-3 de junio], 1994, pp. 91-107. Define documento telemático como "el documento que enviamos o recibimos a través de las telecomunicaciones, es el caso del correo electrónico".

[66] CASELLAS ISERRA, L. E., Arxivistica i noves tecnologies: Consideracions sobre terminología, conceptes i professió, s. l., Ligall, 1999, p. 42.

[67] RENGIFO GARCÍA, Ernesto, "Contratos informáticos y telemáticos" [guía de posgrado], Bogotá, Universidad Externado de Colombia, 1999.

nuestro Código con un criterio ejemplificador de los medios de prueba. El artículo 251 del mismo Código, al definir el documento, concluye "y en general, todo objeto mueble que tenga carácter representativo o declarativo".

2. En la ley 98 de 1993, o Ley del Libro, se señala en su artículo segundo, equiparando las publicaciones tradicionales a las realizadas mediante medios electromagnéticos: "Para los fines de la presente ley se consideran libros, revistas, folletos, coleccionables seriados, o publicaciones de carácter científico o cultural, los editados producidos e impresos en la República de Colombia, de autor nacional o extranjero, en base de papel o publicado en medios electromagnéticos".

3. La ley 270 de 1996, establece por primera vez en la legislación colombiana, el reconocimiento del documento electrónico (validez y eficacia) cuando en su artículo 95 dispone:

> Tecnología al servicio de la administración de justicia: el Consejo Superior de la Judicatura debe propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia. Esta acción se enfocará principalmente a mejorar la práctica de las pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información. Los juzgados, tribunales y corporaciones judiciales podrán utilizar cualquier medio técnico, electrónico, informático y telemático, para el cumplimiento de sus funciones.[68]

4. El decreto 2150 de 1995 en su artículo 26, establece la forma de utilización de los sistemas electrónicos de archivo y transmisión de datos al interior de la administración pública: “Las entidades de la Administración Pública deberán habilitar sistemas de

[68] Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales.

transmisión electrónica de datos para que los usuarios envíen o reciban información requerida en sus actuaciones frente a la administración".

5. Circular del 14 de mayo de 1997 expedida por la Secretaría Jurídica de la Presidencia de la República: en ella se determina que el derecho de petición de los ciudadanos que se realice mediante el uso de las modernas herramientas tecnológicas (Internet, por ejemplo), debe ser asumido como si fuese una petición de la que trata el artículo 23 de la Carta Política.

Con el advenimiento de nuevas tecnologías, el papel tiende al desuso, dando paso al manejo de documentos informáticos, o documentos telemáticos o electrónicos, cuya característica principal radica en contener información en cualquier forma de mensaje de datos. El artículo 6 de la ley 527 de 1999, dispone que "cuando una norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, siempre y cuando la información que contiene sea accesible para su posterior consulta".
Igualmente, el artículo 8 de la misma ley señala que cuando una norma requiera que la información sea presentada en su forma original, ese requisito se satisface si cumple los siguientes requisitos:

- Que pueda garantizarse que la información se ha conservado íntegra desde cuando se generó por primera vez.

- Que al requerirse que la información sea presentada, ésta pueda ser mostrada a quien deba presentarse.[69]

La legislación de 1999 permite distinguir dentro de los mensajes de datos aquellos documentos electrónicos originales, es decir, que pueden reemplazar los escritos originales que suelen

[69] Estos dos requisitos se relacionan directamente con la capacidad de que el mensaje de datos pueda ser almacenado y que además ese almacenamiento implique que el contenido no ha sido alterado, lo que nos pone íntimamente en relación con el tema de las entidades de certificación y los certificados, tratados a continuación.

solicitarse en las relaciones entre particulares o frente al Estado, si cumplen las condiciones que trae la ley. Sin embargo, por economía procesal resulta de mayor valor entender que, salvo la impugnación del documento electrónico original, certificado o no, el juez debe admitirlo como prueba sin hacer elucubraciones extraordinarias al respecto, con lo que convierte a la prueba electrónica en algo imposible.

Adicionalmente, la capacidad de un mensaje de datos para ser prueba judicial o extrajudicial, se encuentra expresamente el artículo 10 de la ley, que dispone lo siguiente:

> Los mensajes de datos serán admisibles como medios de prueba y con la fuerza probatoria otorgada en el Código de Procedimiento Civil a los documentos, recordando que en toda actuación administrativa o judicial no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de mensaje de datos por el sólo hecho de que se trate de un mensaje de datos o por no haber sido presentado en su forma original.

Esta normativa reafirma la relación con el impacto del comercio electrónico en el derecho probatorio. Además, ya no es sólo original el papel escrito, sino, también, el mensaje de datos que tenga las características propias de serlo.[70]

El documento electrónico, para poseer valor probatorio, debe reunir los mismos requisitos de un documento o instrumento *per cartam*, esto es, aquellos requisitos que se refieren a la esencia del documento mismo.

Por la estructura del documento electrónico[71], se puede considerar que el medio más idóneo de prueba en este punto lo constituye el documental, aunque, otro medio probatorio factible de

[70] Resulta fundamental para la anterior concepción la ratificación al concepto de los "equivalentes funcionales" en materia de mensajes de datos según la ley 527 de 1999 efectuada por la Corte Constitucional en sentencia C-662 de 2000. Veamos lo considerado al respecto: "El proyecto de ley, al igual de la ley Modelo, sigue el criterio de los 'equivalentes funcionales' que se fundamenta en un análisis de los propósitos y funciones de la exigencia tradicional del documento sobre papel, para determinar cómo podrían cumplirse esos propósitos y funciones con técnicas electrónicas.

utilización es la prueba pericial, pues se podría convertir la información contenida en el sistema en datos inteligibles, para que el documento llegue al juez de forma tal que facilite su comprensión.

Además, debe tenerse en cuenta que el documento electrónico deberá dar cumplimiento a los requisitos formales instrumentales, esto es, aquéllos establecidos para la validez del acto, y, por lo tanto, en caso de ser necesaria la formalidad por la ley deberá cumplir con las exigencias de la escritura pública, o deberá ser otorgado por funcionario público competente.

Sin embargo, será necesario tener en cuenta que la firma digital, la cual consiste en "Datos asociados con o la transformación criptográfica de una unidad de datos que permite al recipiente probar la fuente y la integridad de la unidad de datos y proteger contra una falsificación", ofrece quizá mayores garantías, aunque en la práctica sea considerada como un mecanismo complejo de seguridad electrónica; además, en la medida en que son varios los intervinientes en la elaboración de la misma se podría pensar en mayor grado porcentual de riesgo al fraude. Lo importante radica, entonces, en que bien sea firma electrónica, definida como "letras, caracteres, números u otros símbolos en forma digital adjuntos o lógicamente asociados con un mensaje electrónico, y ejecutados o adoptados con la intención de autentificar o aprobar el mensaje electrónico", o firma digital, ésta cumpla con las mismas funciones que una firma ológrafa.

Uno de los principios rectores en la interpretación de los documentos electrónicos es el de integridad con el cual se le da plena validez jurídica al documento electrónico en la firma digital o en la firma electrónica como está contemplado en el artículo 7 de la ley 527 de 1999[72].

---

[71] En el proyecto de ley sobre comercio electrónico, el artículo 10 determina que los mensajes de datos son admisibles como medio de pruebas y tendrán la misma fuerza probatoria de los documentos.

[72] RINCON CARDENAS, Erick. Manual de derecho de comercio electrónico y de Internet. Bogotá, Centro Editorial Rosarista, Facultad de Jurisprudencia, 2006. Pág 52.

8. LA CONTRATACION ELECTRONICA

Según definición del tratadista Emilio del Peso Navarro, la contratación electrónica o por medios electrónicos se puede definir como aquella que, con independencia de cual sea su objeto, que también puede ser la informática, aunque no necesariamente, se realiza a través o con ayuda de medios electrónicos que no tienen por qué ser siempre ordenadores. Así, un contrato informático es un acuerdo de voluntades que tiene por objeto bienes y/o servicios informáticos, preceptuado por la teoría general de las obligaciones y los contratos y guiado en lo especial por la informática.

Del Peso Navarro clasifica los contratos informáticos así: contratación del hardware, contratación del software, contratación de datos, contratación de servicios y contratos complejos, con respecto a ello dice que "hasta el presente, el grupo dedicado a los servicios venía siendo una especie de cajón de sastre donde iban a parar todos los contratos que no se referían específicamente al hardware o al software. Así mismo los contratos del tipo de contratación parcial y global de servicios informáticos como outsourcing, o los llamados contratos llave en mano (turn-key package) requieren un tratamiento distinto de los englobados en el anterior grupo de servicios"[73].

El acto jurídico es la manifestación de la voluntad que produce consecuencias jurídicas, e incluye la convención, el contrato y la manifestación unilateral de voluntad. Un acto no jurídico, a contrario *sensu*, es también una manifestación de la voluntad pero que no posee consecuencias jurídicas. El acto jurídico es una de las principales fuentes de las obligaciones. El hecho jurídico es un

[73] DEL PESO NAVARRO, Emilio. Socio Director de Informáticos Europeos Expertos. Contratos Informáticos. Internet, Lima.

acontecer de la naturaleza que produce efectos jurídicos y además es independiente de la voluntad humana.

El contrato en línea se celebra en interpartes a través de una red, *id est*, por personas presentes pero interactuando a través de un medio telemático. La oferta y la aceptación se realizan por correspondencia, se define dónde, en qué lugar se entiende perfeccionado el contrato. Se presume que el oferente ha recibido la aceptación cuando el destinatario pruebe la remisión de ella dentro de los términos fijados por los artículos 850 y 851 del Código de Comercio

Según la doctrina, el perfeccionamiento del contrato por correspondencia se da en dos posiciones, una en el momento en que el destinatario manifieste su voluntad aceptando la oferta como cuando contesta, en cuyo caso el lugar de celebración del contrato será el del domicilio del aceptante y la de la expedición de la declaración de voluntad, y otra donde el contrato se perfecciona en el momento en que la respuesta que contiene la aceptación es expedida o enviada al oferente. Nuestro Código del Comercio, adopta el sistema de la recepción, con finalidad probatoria[74].

8.1. Etapa precontractual.

Es en el periodo precontractual donde se delimita y precisa el objeto de la prestación del servicio, en donde el usuario describe sus necesidades y la reciproca conducta del proveedor en cuanto al cumplimiento de sus deberes de información y consejo, a fin de mantener el equilibrio entre los contratantes. La adecuada información y consejo por parte del proveedor de bienes y servicios informáticos, representa un papel protagónico en esta etapa precontractual, lo

[74] TORRES TORRES, Henry William. Derecho informático.Bogotá. Ediciones Jurídicas, 2002.Pág 94.

que constituye un derivado del deber de comportarse de buena fe en las diversas fases del inter contractual, comenzando por las tratativas previas, lo que en nuestro derecho encuentra sustento en el artículo 1198 del Código Civil.[75].

Sin embargo, es el usuario el responsable de establecer el contenido del requerimiento efectuado al proveedor basado en el claro conocimiento de sus necesidades. De Lamberterie sostiene que, un estudio deficiente trae como consecuencia la elección de un sistema inadecuado del usuario que no ha analizado sus necesidades y que deberá tolerar las consecuencias de esa elección defectuosa.

Los tribunales galos, hasta 1979 sostuvieron que solo el cliente era responsable si no había hecho un análisis profundo de sus necesidades, criterio que fue modificado por la Corte de París en un pronunciamiento del 3/4/79, donde señala que pertenece al cliente definir sus necesidades y los objetos a alcanzar, formulando claramente la naturaleza y el volumen del trabajo a automatizar, además señala que sobre el proveedor pesa una clara obligación de ayudar al cliente a expresar sus necesidades, así, la obligación de informar del usuario se equilibra con la del fabricante de informar y aconsejar.

El artículo 14 de la Ley 527 de 1999 se refiere a la formación del contrato: *"En la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos".*

Luego, se concluye que la oferta a través de un mensaje de datos es válida a menos que las partes pacten que la oferta y su aceptación no serán válidas

[75] TORRES TORRES, Op cit. Pág 96

cuando se manifiesten por medio de un mensaje de datos. Una vez comunicada la oferta, ésta se hace irrevocable y al ser aceptada se gesta el contrato. Por consiguiente, una vez comunicada, no podrá retractarse el proponente, so pena de indemnizar los perjuicios que con su revocación cause al destinatario"[76].

8.2. Etapa contractual.

Un contrato tiene como finalidad restringida la creación de obligaciones, así el contrato electrónico es solo una forma de designar un contrato que se celebra con la participación de medios electrónicos. Todo contrato que se oficie por cualquier medio de comunicación, está compuesto de una oferta (emisor, iniciador) y una aceptación (receptor, destinatario).

En cualquier caso, sitios web mediante los chats o video conferencias, correo electrónico (e- mail) o los "clic wrap agreements", se vincula por lo menos a dos sujetos, uno cumpliendo el rol de oferente y el otro el de aceptante, sin efectuar una comunicación completamente directa sino que se sirve de medios electrónicos, sin que por esta circunstancia se le reste eficacia jurídica al contrato celebrado a través de la Internet.

El derecho estima que solo las relaciones libres son realmente eficaces y todas las soluciones legales propender por mantener ilesa tal libertad, la cual se manifiesta en la voluntad consciente, seria y estable dirigida a producir efectos jurídicos, incluso en Internet.

Así, con el objeto de definir y reglamentar "el acceso y uso de los mensajes de datos, del comercio electrónico y las firmas digitales" entre otros, se expidió la

[76] BOTERO Y OTROS, Op. Cit . Pág 39

Ley 527 de 1999, que en su artículo 2, literal b) definió comercio electrónico como las *"cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o cualquier otro medio similar".* Disposiciones que son entendidas como la derogación de la normatividad general,-Código del Comercio y Código Civil-, por resultar inaplicables.

Sin embargo la propia ley admite regulaciones diferentes a las proferidas en la Ley 527 de 1999, el artículo 4 in fine, le confiere el carácter supletivo a las normas contenidas en el capítulo III de la parte I de la ley, que se refiere a la comunicación de los mensajes de datos, acogiendo el que se puede disponer de las normas generales.

Igualmente, el artículo 22 de la misma Ley, establece que los efectos de los negocios jurídicos que se celebren mediante mensaje de datos *"se regirán conforme a las normas aplicables al acto o negocio jurídico contenido en dicho mensaje de datos"* subsistiendo la aplicación de la normatividad general en cuanto a las obligaciones y su cumplimiento.

El artículo 44 in fine establece la figura de la incorporación por remisión, donde las partes pueden hacer una remisión total o parcial a "*normas, directrices, estándares, acuerdos, cláusulas, condiciones o términos fácilmente accesibles con la intención de incorporarlos como parte del contenido o hacerlos vinculantes jurídicamente",* además señala que los términos serán jurídicamente válidos *"entre las partes y conforme a la ley"*[77].

De manera tal, que la ley 527 de 1999, de comercio electrónico presenta grandes vacíos, por cuanto no manifiesta expresamente los principios que

[77] BOTERO, Luís Felipe y otros. Comercio electrónico en Colombia. Principales aspectos legales. Primera edición. Bogotá, Baker & McKenzie, 2002. pág 36.

inspiran dicha ley como usualmente ocurre en nuestra legislación, adicionalmente no reguló a cabalidad el tema de la formación de la voluntad como paso previo para el contrato electrónico, razón por la cual es necesario regularse con la legislación mercantil. La ley 527 no reguló como tal los requisitos o elementos que deben reunir la oferta y la aceptación, solo su validez cuando es expresada como mensaje de datos.

8.2.1. Elementos esenciales del contrato

Los elementos esenciales de un contrato corresponden a aquellos que generan la validez de un acto jurídico como son: Capacidad legal, consentimiento libre o sin vicio, objeto lícito y causa lícita, en concordancia con el artículo1502 del Código Civil, donde establece que, para que una persona se obligue frente a otra por un acto o declaración de voluntad es necesario: a) Que sea legalmente capaz. b) Que consienta en dicho acto o declaración y que su consentimiento no adolezca de vicio. c) Que recaiga sobre un objeto lícito. d) Que tenga causa lícita.

a). La capacidad. Se ha definido como la aptitud de una persona para ser titular de derechos y para ejercerlos, sin el ministerio o la autorización de terceros. Sin embargo, todas las personas por el solo hecho de existir, son titulares de derechos, es decir, son jurídicamente capaces. Sin embargo, la capacidad de ejercicio, consiste en la aptitud de una persona para ejercer por si misma derechos y contraer obligaciones. Así, todas las personas pueden ser titulares de derechos pero no todas pueden ejercerlos[78]. Los actos realizados por estos incapaces están sancionados con la nulidad absoluta.

[78] TORRES TORRES, H. Op cit. Pág 101.

b). El consentimiento. Se entiende por consentimiento la intención común de los contratantes, su acuerdo de voluntades, o la voluntad de la persona que se obliga. Es así, como al hablar sobre la obligatoriedad del contrato el consentimiento se constituye en el elemento sobre el cual se basa la validez del acto jurídico celebrado. El consentimiento por si solo sin necesidad de formalismos, es capaz de obligar, es eficaz para perfeccionar el contrato.

c). El objeto lícito. Otro de los requisitos exigidos por el artículo 1502 del C.C. para la validez del acto jurídico se refiere al objeto lícito. Al respecto, el artículo 1517 del C.C. dispone: "toda declaración de voluntad debe tener por objeto una o más cosas que se trata de dar, hacer o no hacer. El mero uso de la cosa o su tenencia puede ser objeto de la declaración"[79].

Por objeto del contrato se entiende el tipo de operación jurídica que las partes escogen como reguladora de su negocio jurídico, como es una venta, una sociedad. Por objeto de la obligación, se entiende la prestación o prestaciones que las partes salen a deber y que se originan en el tipo de contrato que se celebró.

d) La causa. Para dar validez al acto jurídico, el artículo 1502 del Código Civil exige como cuarto elemento, la causa. Lo cual se fundamenta en el artículo 1524 de la misma norma: "No puede haber obligación sin una causa real y lícita. Pero es necesario expresarla". Se entiende por causa el motivo que induce al acto o contrato, y por causa ilícita la prohibida por la ley, o contraria a las buenas costumbres o al orden público. De tal manera que la promesa de dar algo en pago de una deuda que no existe, carece de causa, y la promesa de dar algo en recompensa, de dar algo por un crimen o de un hecho inmoral tiene una causa

[79] Ibídem. Pág 109.

ilícita. En relación con cualquier acto jurídico son muchas las razones o motivos que pueden explicar o, que pueden considerarse como su causa.

8.2.2. Momento y lugar de celebración del contrato electrónico.

Un punto álgido en la celebración de un contrato electrónico consiste en determinar el momento y el lugar del acontecimiento, para lo cual la Ley 527 en su artículo 25 dispuso:

> *"Lugar del envío y recepción de mensajes. De no convenir otra cosa el iniciador y el destinatario, el mensaje de datos se tendrá por expedido en el lugar donde el iniciador tenga su establecimiento y por recibido en el lugar donde el destinatario tenga el suyo. Para los fines del presente artículo:*
> *a) Si el iniciador o destinatario tienen más de un establecimiento, su establecimiento será el que guarde una relación más estrecha con la operación subyacente o, de no haber una operación subyacente, su establecimiento principal,*
> *b) Si el iniciador o el destinatario no tiene establecimiento, se tendrá en cuenta su lugar de residencia habitual.*[80]"

Por tanto el contrato se entiende celebrado en el momento en que el oferente reciba la aceptación, en los términos del artículo 24 de esta ley. Luego, las obligaciones que surgen del contrato electrónico se rigen por las normas especiales del respectivo contrato y las generales de todo contrato, como lo establece el artículo 22 de la Ley 527 de 1998. En el mismo sentido, la responsabilidad por incumplimiento de las obligaciones se regirán por las normas generales.

[80] BOTERO y otros. Op. Cit. Pág 46.

8.2.3. Clasificación.

El Comercio Electrónico, o e-busines, e-comerce, e-banking empezó a ser definitivo en la economía; con la llegada de la Internet a nuestro país, muchos colombianos emprendedores montaron tiendas virtuales o negocios minoristas en Internet. Empresas grandes, pequeñas y medianas consideraron la posibilidad de realizar negocios por Internet, entidades bancarias ofrecieron servicios financieros operativos por esta vía, como valor agregado para sus clientes. El comercio electrónico se puede clasificar en: de negocio a negocio, de consumidor a empresa, de empresa a consumidor, y entre consumidores.

8.2.3.1. Comercio electrónico negocio a negocio.

La actividad comercial electrónica de negocio a negocio, se encuentra reflejada en aquella relación de intercambio de bienes y servicios entre empresas. Se trata de organizaciones que llevan a cabo actividades económicas que tienen como particularidad una gran magnitud de transacciones; negocios en los cuales se da aplicación de certificados digitales y otros medios de autenticación.

Esta operación no podría ser llevada a cabo sin un sistema cerrado y que brinde seguridad y confianza de la transferencia de datos entre las empresas participantes, conocido como intercambio electrónico de datos o EDI.

8.2.3.2. Comercio electrónico de consumidor a empresa.

Es la forma de comercio electrónico en la que el usuario es quien realiza la operación mercantil dejando claras las condiciones propias de ésta. Esta operación mercantil se ve en la compra de tiquetes aéreos en donde es el cliente

de la aerolínea mercantil quien elige destino fecha y hora en que desea adquirir el servicio de la empresa aviadora.

8.2.3.3. Comercio electrónico de empresa a consumidor.

Este tipo de operaciones se dan desde la entrada del Internet y de los sistemas de interconectividad global, siendo una manera eficaz de realizar transacciones sobre bienes de una forma masiva. Corresponde a aquellas operaciones de suministro de bienes y servicios que hacen las empresas que forman parte en el mercado, a los consumidores; lo cual es una realidad de diario acontecer con las facilidades que brindan los medios electrónicos de acceder a los productos y servicios.

8.2.3.4. Comercio electrónico entre consumidores.

Este modo de comercio electrónico es realizado con intervención de terceros, los cuales cobran un porcentaje en la operación comercial realizada entre las partes y prestan un método para regular las transacciones y el cumplimiento de las partes que participan, a través de la creación de páginas Web, a las cuales pueden acceder tanto oferentes comunes como posibles compradores, en la modalidad de remates o subasta en la cual los mismos consumidores son los que realizan sus actividades comerciales en lo que atinente a transacciones monetarias; este hecho es hoy en día común entre quienes navegan en la red, en busca de precios más accesibles y no siempre en busca de obtener productos nuevos, sino que también representa una posibilidad adquirir productos usados y que se encuentran en condiciones optimas para el uso. En realidad, el Comercio Electrónico en Colombia requiere de un mayor compromiso por parte del Estado, mejorando la infraestructura de telecomunicaciones y el fácil acceso a Internet, como estímulo a este tipo de actividad económica del país.

8.2.3.5.- Directos e indirectos

Otra clasificación del comercio a través de medio electrónico, hace referencia a los bienes y servicios que son acordados comerciar, producto de una operación electrónica, y la entrega de éstos puede ser directa e indirecta.
La forma directa de llevar a cabo esta operación, se da por el surgimiento de una transacción completa efectuada por vía electrónica; la cual comprende desde el momento en que es realizado el pedido hasta el momento del pago y entrega en línea por medio del sitio web, realizando operaciones en gran serie de bienes y servicios que no resultan ser tangibles. Un ejemplo es el caso de las recargas de teléfonos celulares por vía electrónica, la cual comprende desde la solicitud de la recarga hasta el pago de la misma, que se realizan desde el portal web.

El modo indirecto, es aquel en el cual la solicitud o requerimiento de un producto, bien o servicio se realiza por medios electrónicos, sin embargo su distribución o suministro son realizados por los medios habituales de entrega física. A manera de ejemplo podemos encontrar los casos de la venta de diferentes productos por Internet, el caso de las tele ventas, circunstancias en las cuales las mercaderías son solicitadas mediante algunos de los medios electrónicos, ya sea el Internet, el teléfono o el fax, pero la entrega real y material del producto se realiza por los típicos medios de mensajería.

Sea cual sea la actividad comercial ejercida, ya sea una operación de empresa a empresa, o de consumidor a empresa o cualquier otra forma para llevarla a cabo, el uso de los medios electrónicos, marca una nueva era y una nueva forma de ejercer el comercio, y trae consigo ventajas y beneficios para las diferentes partes contratantes.

9. LOS DELITOS INFORMATICOS.

Algunas definiciones de delitos informáticos, hechas por expertos son:

"Todo comportamiento antijurídico, no ético o autorizado, relacionado con el procesamiento y transmisión de datos"[81].

"Los delitos informáticos son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)"[82]

Para el tratadista italiano CARLOS SARZANA:

"Los delitos informáticos son cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo"[83]

En este sentido es claro concebir el delito informático como un acto que implica una conducta punible, es decir atípica, antijurídica y culpable, para la cual se prevé una sanción penal drástica debido a que se lesionan intereses individuales y sociales relacionados con los miembros de una colectividad.

En este sentido, los delitos informáticos son actos que permiten la comisión de agravios, daños o perjuicios en contra de las personas, grupos de ellas, entidades o instituciones y que por lo general son ejecutados por medio del uso de computadoras y a través del mundo virtual de Internet.

---

[81] RIVERA LLANO , Abelardo. Dimensiones de la informática en el Derecho. Pág 82
[82] TELLEZ VALDEZ, Julio. Derecho informático. Ciudad de México, D.F., MacGraw Hill, 1996. Pág 104.
[83] SARZANA, Carlos, Criminalità e tecnología, citado por PEÑA, PALAZUELOS y ALARCON, publicación en Internet en: http:unam.edu.mx, p.1.

A su vez los delitos informáticos pueden comprender tanto aquellas conductas que recaen sobre herramientas informáticas propiamente, como aquellas que valiéndose de estos medios lesionan otros intereses jurídicamente tutelados como son la intimidad, el patrimonio económico, la fe pública, entre otros.

Los delitos informáticos comprenden: virus, gusanos, bombas lógicas o cronológicas, sabotaje informático, piratas informáticos o hackers, acceso no autorizado a sistemas o servicios, reproducción no autorizada de programas informáticos de protección legal, manipulación de datos de entrada y/o salida, manipulación de programas, fraude efectuado por manipulación informática.

En Colombia, la ley 1273 de enero de 2009, sancionada por el Presidente Álvaro Uribe Vélez, por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico denominado 'De la protección de la información y de los datos', se establece que el ciudadano que, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de 48 a 96 meses, y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP (Protocolo de Internet) diferente, en la creencia de que acceda a su banco o a otro sitio personal o de confianza.

En su primer capítulo, la norma dicta medidas penales de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. La norma tiene en cuenta:

*Acceso abusivo a un sistema informático: habla del acceso parcial o completo a un sistema informático protegido o no con una medida de seguridad.

*Obstaculización ilegítima de sistema informático o red de telecomunicación: quien obstaculice el normal funcionamiento o acceso a un sistema informático o a una red de telecomunicaciones.

*Interceptación de datos informáticos: quien sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.

*Daño informático: quien destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.
*Uso de software malicioso: quien distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

*Violación de datos personales: quien obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Con esta reglamentación Colombia da un paso muy importante en este tema legal, pero no se debe olvidar que en el mundo de la tecnología hay tanta dinámica, que si con esta modificación del Código Penal no se consideran las posibles nuevas modalidades que van a surgir y se permita que queden sin castigo, este proyecto de ley quedará a medias. Es importante que sea lo

suficientemente flexible para poder acoger lo que viene en el futuro del cibercriminalismo. Si no lo es, en poco tiempo quedará obsoleta.

En Colombia el fraude informático apenas comienza a ser una amenaza para el actual sistema legislativo. Nuestro derecho no cuenta con figuras penales específicas que abarquen las actividades ilícitas que se puedan lograr por medio de la informática; se cuenta con conductas sancionables por no ser éticas pero carentes de regulación, elemento indispensable para la existencia del delito. Pues nuestro ordenamiento jurídico regula de una manera muy global el delito informático:

La Constitución Política de Colombia[84] en su artículo 15 consagra el derecho a la intimidad, establece que *"todas las personas tiene derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar…".* El mismo artículo establece que: *"…La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley…".*

- El Código Penal (Ley 599 de 2000) en su artículo 192 establece la violación ilícita de comunicaciones y determina que: *"el que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido incurrirá en prisión…"* además agrava la pena cuando *"…el autor de la conducta revela el contenido de la comunicación, o la emplea en provecho propio o ajeno o con perjuicio de otro…".* Esta norma se convierte en una herramienta de gran importancia en defensa de los derechos para el control de la información ante medios informáticos.

[84] CONSTITUCION POLITICA DE COLOMBIA. Editorial Temis de Santafe de Bogotá, 1991.

- El artículo193 del mismo Código establece pena de multa por ofrecimiento, venta o compra de instrumentos empleados para interceptar la comunicación privada entre personas, pues solo el Estado tendría tal derecho con una autorización judicial previa.

- El Código Penal en su artículo 194, sanciona con multa la divulgación de documentos que por su naturaleza deban permanecer bajo reserva. Esta norma también protege el derecho a la intimidad.

- El artículo 195 del Código Penal, sanciona con multa *"el que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo…".* La importancia de este artículo consiste en que a pesar de ser un delito penalizado con multa, se sanciona de manera genérica el delito informático como tal.

- El artículo 196 del Código[85] en mención, sanciona con prisión la violación ilícita de comunicaciones o correspondencia de carácter oficial, como necesidad que tiene el gobierno de proteger su información.

- Igualmente, el artículo 197 regula la utilización de equipos transmisores o receptores de señales, sancionando con prisión al que los utilice o los posea con fines ilícitos, la pena se agrava si el que los utiliza o los posea tenga fines terroristas.

Finalmente, el artículo 272 del Código Penal, sanciona con multa la violación a los mecanismos de protección de los derechos patrimoniales de autor, como son: la violación a las medidas tecnológicas adoptadas para restringir los usos no autorizados; la supresión o alteración de la información esencial para la gestión electrónica de derechos; y la fabricación, importación, venta, arriendo o

[85] CODIGO PENAL de 2000, artículo 196 , santafé de Bogotá, Legis, 2001.

cualquier forma de distribución al público de dispositivos o sistemas que permitan descifrar una señal de satélite portadora de programas, sin autorización del distribuidor legítimo de esa señal.

Como podemos ver, en nuestra legislación se ha venido creando un Derecho preinformático, con la expedición de normas, decretos, resoluciones, circulares, sobre sistemas de información y procesamiento de datos, transmisión y recepción de información codificada, políticas en sistemas de información, programas de información para el sector público, inscripción del soporte lógico, servicios informáticos y de telemática, investigación científica y tecnológica, información en soporte magnético, libros de comercio etcétera, etcétera, sin embargo en el terreno de lo penal, la Ley 599 de 2000 -Nuevo Código Penal- apenas se incluye algunos aspectos generales, con pequeñas sanciones y deja por cubrir grandes vacíos, lo que proyecta una necesidad urgente de introducir en el derecho penal vigente una tipificación básica de los delitos informáticos en general.

Es así, como a la aplicación del Código Penal se argumenta tan solo una atipicidad relativa lo cual vulnera el principio de la legalidad, pilar de nuestro derecho penal, en el sentido de que se afirma que no existen delitos informáticos en sí, sino conductas no éticas y antijurídicas cuyos medios de ejecución son las computadoras o las redes con total desconocimiento de la clasificación técnica de estas conductas criminales.

Sin lugar a dudas, la informática se ha convertido en un factor determinante del origen de nuevas formas delictivas que tienen como medio y objeto una computadora. Esta es la contraposición a los grandes beneficios que la informática ha aportado a sectores como el periodístico, el financiero y judicial.

Estas nuevas formas delictivas desestabilizan las actuales estructuras jurídicas en el campo penal, las cuales no están preparadas para hacerle frente a estos nuevos hechos sociales, razón por la cual los legisladores se encuentran en la obligación de tipificar los nuevos hechos punibles, colocando a la ley a la par con la tecnología y así el Derecho Penal pueda dar respuestas en justicia, cumpliendo además con el principio *nullum crime sinne lege previa penale*[86].

En algunos países productores como Estados Unidos, Japón, Corea, India y del bloque europeo, son muy altos los índices de criminalidad informática, y tienen como característica que las infracciones en su gran mayoría son cometidas por personas de confianza, con conocimientos técnicos especializados, hechos punibles conocidos como *computer crime,* los cuales sí están tipificados como delitos.

El profesor CARLOS SARZANA, estudioso de los delitos por computadora considera que: "La evolución de las nuevas tecnologías ha traído consigo una nueva forma de criminalidad -*white collar*- que tiene por objeto y por instrumento indiscutible la computadora, siendo esta un refinado producto del progreso tecnológico en el campo de los negocios. Teniendo en cuenta el elevado *dark number* y la naturaleza devastadora de sus consecuencias, es cierta la peligrosidad social de tales formas de criminalidad". Y agrega: "No nos dejemos emocionar demasiado por la aparición de estas formas de criminalidad al punto de olvidar que por esto van a dejar de ser más peligrosas"[87].

Como ya se había mencionado, la información, dentro de una sociedad tecnológica, se ha convertido en un bien jurídico, con las reservas de que sea un bien inmueble merecedor de tutela legal, al cual las leyes vigentes tanto en

[86] LEON MONCALEANO, W. Op Cit. Pág 162.
[87] SARZANA, Carlos. Note Sul Diritto Penale dell´informática. Giust Penale.1984

materia civil como penal no le dieron protección porque consideraron que la información y el poder que representa no eran susceptibles de ataques y que el transporte de ella estaba dentro de la ciencia ficción o que ya estaba salvaguardada con la protección de la fe pública o el derecho a la información. Sin tener en cuenta que los impulsos magnéticos contenidos en una cinta pueden ser copiados fraudulentamente, saboteados, robados sus servicios, de manera tal que con una tecnología avanzada se puede revisar una entidad bancaria con todos sus movimientos financieros. El manejo de toda esta información obliga necesariamente a pensar en la protección de este bien.

Una forma jurídica *sui generis* de aplicación a toda actividad contraria al derecho en lo referente a la informática, se concreta como delito a distancia, en donde por no dejar sin castigo estas conductas, los jueces y fiscales aplican otras normas de adecuación típicas que van en contravía de los principios del Derecho Penal, lo que conlleva a sugerir a los legisladores la creación de nuevos tipos penales o una ley independiente de informática.

Entonces, el ilícito informático se caracteriza por:

- Ser un delito eminentemente doloso, su actor lo realiza con la intención de dañar, o atacar los sistemas de computación, o utiliza a la computadora como medio para cometer otros ilícitos. De tal manera que al darle el trato de un delito eminentemente doloso y no de mera contravención, puede ser investigado por la Fiscalía General como titular de la acción penal de oficio o a través de las denuncias de los particulares afectados. Y como existe responsabilidad tanto civil como penal en la comisión del hecho punible informático, existe la obligación de indemnizar los perjuicios ocasionados por la conducta para resarcir los daños inferidos a quienes hayan sufrido detrimento con su ejecución.

- Ser un delito de cuello blanco (*white collar crimes*), implica hechos punibles o delitos que solo pueden ser ejecutado por un grupo determinado de personas pues su comisión requiere de una preparación y conocimientos específicos sobre el tema. Según concepto del magistrado de la Corte Suprema, NILSON PINILLA es el "crimen organizado", pues se trata de delitos cometidos por un sujeto activo cualificado por la naturaleza de sus conocimientos generales de informática y muy particular en el sistema informático que pretende defraudar.[88]

Y más aún, para la comisión del delito informático, su autor debe determinar cual es el momento más favorable para actuar, lo que algunos autores llaman "deshonestidad latente del criminal informático" que espera que la ganancia sea proporcional al riesgo que implica el fraude. Además son acciones que se pueden consumar en milésimas de segundo por lo cual ofrecen facilidades de tiempo y espacio para su ejecución, sin que necesariamente haya presencia física en el ámbito de los sujetos pasivos.

Estos delitos son muy pocas veces denunciados, lo que hace que las autoridades por desconocerlos no los investiguen formando parte de lo que en criminología se conoce como la "cifra oscura", o dorada de la delincuencia, en parte porque sus actores generalmente pertenecen a los círculos políticos o financieros, por lo que sus conductas son socialmente aceptadas lo que impide el ejercicio del *ius puniendi* del Estado. Como son delitos que conllevan grandes pérdidas económicas o perjuicios deberían indicarse en las normas tipificadoras[89].

[88] LEON MONCALEANO, W. Op Cit. Pág 168.
[89] Ibídem. Pág 170.

Los delitos informáticos de ordinario se cometen a nivel nacional o local, sin embargo con la existencia de los sistemas informáticos de utilización integral y debido a que adquieren un alcance internacional, se convierten en delitos informáticos internacionales, para los que su penalización se requiere recurrir a la celebración de tratados internacionales entre los estados o la aplicación de los conceptos de la ley penal en el tiempo y en el espacio.

El Código Civil en su artículo 1494 en concordancia con los artículos 2341 y 2356 establecen que el delito es fuente de las obligaciones, en armonía con el artículo 103 del Código Penal y 94 que reitera que de los delitos nacen las obligaciones de reparar los daños materiales y morales que de ellos provengan. De manera que al cometerse un hecho punible informático se deben indemnizar daños y perjuicios por los que resulten penalmente responsables y aún en forma solidaria (Arts. 105, 106 y 107 C. P., en consonancia con los artículos 95 y 96 de la citada ley), a favor de la persona natural o jurídica que haya resultado perjudicada[90].

Cabe anotar que la responsabilidad se puede clasificar en contractual, cuando la persona está en la obligación de resarcir el daño causado en razón de una relación contractual en la que se haya verificado el incumplimiento por parte del deudor, y en extracontractual cuando independientemente de esa relación contractual la persona debe responder patrimonialmente por un acto, omisión u otro hecho. Estos dos tipos de responsabilidad son aplicables en materia de informática.

Según criterio de los autores MARIA FERNANDA GUERRERO MATEUS y JAIME EDUARDO SANTOS MERA, la actividad informática es una actividad peligrosa a la que se le deben aplicar todas las doctrinas y jurisprudencias emanadas del

[90] LEON MONCALEANO, William Fernando, Op cit, pág 171.

artículo 2356 del Código Civil colombiano, fundamentalmente lo referente a la presunción de culpa en el agente causante del daño que implica por lo mismo un relevo en la carga de la prueba para la persona afectada[91]. Esta serie de conductas eminentemente constitutivas de delitos informáticos, los *computer crimes,* atentan directamente contra el orden económico y social.

9.1.CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.

9.1.1. Delitos de violación a la intimidad y otras garantías.

9.1.1.1. Violación ilícita de comunicaciones.

El artículo 192.-Violación ilícita de comunicaciones, expresa: El que ilícitamente sustraiga, oculte, extravíe, destruya, intercepte, controle o impida una comunicación privada dirigida a otra persona, o se entere indebidamente de su contenido, incurrirá en prisión de uno (1) a tres (3) años, siempre que la conducta no constituya delito sancionado con pena mayor.

Sujeto activo. Es indeterminado.
Sujeto pasivo. Son el emisor y el receptor de la información. En caso de presentarse interceptación de línea telefónica para obtener los datos enviados, no se puede generar una adecuación típica porque no hay comunicación teóricamente hablando y la conducta sufriría el fenómeno de la atipicidad relativa.
Objeto jurídico. En sentido amplio son las comunicaciones privadas y en sentido estricto es la información.

[91] GUERRERO MATEUS, María Fernanda y SANTOS MERA, Jaime Eduardo. Fraude Informático en la Banca. Pág 75.

Objeto material. Es la información como bien privado.
Conducta. Contiene varios verbos rectores: sustraer, ocultar, extraviar, destruir, interceptar, controlar, impedir y enterarse. Sustraer es apropiarse de la comunicación, interceptarla, desviarla de su curso regular, dañar, propagarla, emplearla en provecho propio o ajeno.

La comisión de este delito es propiamente informático, ya que está dirigido a la violación del objeto material que es la información, como la interceptación de llamadas telefónicas, interceptación del correo electrónico o *e-mail,* entre otros.

9.1.1.2. Acceso no autorizado a sistema de procesamiento de datos.

Está constituido por todas aquellas conductas delictivas cometidas a través de las computadoras con el fin de acceder ilegalmente a cualquier sistema de procesamiento de datos en forma remota. El artículo 195 del Código Penal al respecto expresa: "El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa". Lamentablemente este es el único delito informático tipificado en el nuevo Código Penal con una redacción tan superficial que denota el desconocimiento de la inmensa gama de delitos informáticos que se pueden presentar, y debido a la tipificación tan restringida la cadena de conductas que quedaron por fuera habrán de concurrir con otros delitos.

La norma trae un elemento subjetivo que es el vocablo "abusivamente", donde simplemente debió decir "el que se introduzca", dejando de lado el elemento subjetivo, el cual puede ser tomado por el usuario de la computadora como sujeto activo o por cualquier sujeto de cuello blanco como argumento que estaba en otra red, que navegaba o tuvo algún acceso así fuera fortuito, pues es claro que si el

delito es eminentemente doloso se descarta una intromisión hecha por error o en forma negligente a un sistema[92].

Sujeto activo. Es no calificado o indeterminado. Básicamente se refiere a los piratas informáticos *hackers,* sujetos que por su alto coeficiente intelectual y su habilidad en el manejo de sistemas informáticos se crean retos para acceder a sistemas protegidos con complejas medidas de seguridad.
Sujeto pasivo. Puede ser cualquier persona dueña de un sistema de procesamiento de información.
Objeto jurídico. Es la información genéricamente considerada. La conducta es antijurídica ya que se accede a un conjunto de datos almacenados por el titular y es dicha información lo que el derecho busca proteger.
Objeto material. La protección de los sistemas informáticos, pero en concreto la protección a los mecanismos que permiten o restringen el acceso al sistema.
Conducta. El verbo rector es introducir, que significa entrar en un lugar, sin embargo el verbo correcto debió ser acceder que implica abrir, entrar y atravesar.
Este tipo de delito tiene dolo genérico, excluyendo los denominados dolos específicos, pero es claro que el delincuente informático sí tiene un dolo específico, pues el ingreso a un sistema o a una computadora ajena tiene como objetivo destruir información, dañar el sistema, alterar la información, o tomar la información con fines ilícitos, la verdadera intención del *hacker* no es la de acceder por acceder.

Igualmente, la norma exige que "esté protegido con medida de seguridad", lo que significa que si el sistema no está protegido no hay delito?. Es evidente que una persona que ingresa a cualquier sistema en red o no de tipo informático, con dolo cualificado como genérico o como específico se le debe sancionar la verdadera intención imponiendo la pena privativa de la libertad.

[92] LEON MONCALEANO, W. Op Cit. Pág 200.

9.1.2. Delitos contra la libertad de trabajo y asociación.

9.1.2.1. Sabotaje informático.

Consiste en la destrucción o el apoderamiento de los centros neurálgicos computarizados, para que el sistema solamente le obedezca al intruso o se caiga cuando el así lo desee.

El Nuevo Código adoptó el término incluyendo los sistemas informáticos así:
Artículo 198.-Sabotaje. El que con el fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, equipos o materias primas, incurrirá en prisión de uno (1) a seis (6) años y multas de cinco (5) a veinte (20) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.

Sujeto activo. Es no calificado o indeterminado. Tiene un elemento subjetivo que consiste en la intención de paralizar o suspender la actividad laboral, así el delito que se adecuaría típicamente sería el de daño.

Sujeto pasivo. Desde una visión estricta, el afectado es el empleador que es quien sufre el detrimento patrimonial y desde el punto de vista genérico el sujeto pasivo es el Estado ya que el bien jurídico tutelado o dañado es la libertad de trabajo, valor fundamental considerado en nuestra Constitución en los artículos 2, 53 y 54.

Objeto jurídico. Puede ser el patrimonio económico, o el orden económico social o la libertad de trabajo sin ser excluyentes mutuamente.

Objeto material. Desde el punto de vista informático, está dirigido a proteger la información ya que es un bien privado fundamental para la ejecución de ciertas

actividades laborales y junto con los equipos de procesamiento de datos se ha convertido en uno de los más preciados bienes dentro de la economía actual.
Conducta. Contiene varios verbos rectores: destruir, inutilizar, desaparecer y dañar. Destruir alude a deshacer, arruinar o asolar una cosa material o inmaterial[93], inutilizar es hacer que una cosa material e inmaterial no produzca ningún provecho, fruto o interés; dañar es causar detrimento, perjuicio, menoscabo, dolor o molestia.

9.1.3. Delitos contra el patrimonio económico.

9.1.3.1. Hurto informático.

Los artículos 349, 350 y ss. del C. P. y los artículos 239, 250 y ss. Nuevo Código Penal, se refieren al apoderamiento o sustracción de bienes informáticos de naturaleza mueble, como delito que atenta contra el patrimonio económico, con el propósito de obtener un provecho ilícitamente, lo que comprende conductas como el hurto del *hardware, software,* microcircuitos de computadoras, o microchips y demás accesorios que por sus elevados valores en el comercio debería tener unas penas altas.

Sin embargo el verdadero hurto informático está relacionado con la sustracción de información o el apoderamiento de otros bienes, como dinero o mercancías a través de las computadoras, cuan do su entrega está controlada por la propia máquina y comprendería el uso de las claves lógicas, que hay en día se contempla como hurto calificado según lo establecido en el inciso 4 del artículo 350 del Código Penal, al establecer la calificación y aumento de pena si se comete: “Con escalamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes”.

[93] Diccionario de la Real Academia Española, vigésima primera edición, Madrid, 1992, pág 734.

Sujeto activo. Es indeterminado, puede ser cualquier persona natural. El sujeto activo tiene como elemento subjetivo el buscar provecho para si o para un tercero.
Sujeto pasivo. Es igualmente indeterminado. Las victimas pueden ser personas tanto naturales como jurídicas propietarias o poseedoras de dicho bien.
Objeto jurídico. Es el patrimonio económico privado, no exclusivamente a la propiedad sino a todas las instituciones jurídicas que conforman el patrimonio.
Objeto material. Son las cosas corporales muebles que según la legislación civil "pueden transportarse de un lugar a otro, sea moviéndose ellas mismas,…, sea que solo se mueven por fuerza externa,…"[94].
Conducta. El verbo rector en la conducta es apoderarse, que significa sustraer, sacar de la esfera del dominio, tomar sin derecho[95]. Este es un delito de resultado, ya que necesita del apoderamiento de la cosa.

Sin necesidad de usar armas de fuego para robar un banco, sin asaltar carros transportadores de valores, simplemente con un click, los delincuentes informáticos están desocupando cuentas bancarias en cinco minutos y están hurtando el dinero de inocentes ahorradores. Se ha constatado, cómo desde un café Internet, aprovechando la libertad que brindan estos establecimientos para insertar discos compactos (CD) en los computadores se cometen estos actos ilícitos.

CASO

Un sujeto. No fue a la universidad y se dedica al rebusque. En su andar aprendió los secretos del hurto informático. De manera clandestina e ilegal, compra en el mercado informal un programa computarizado (software). Se trata de suplantaciones de las redes informáticas bancarias, que son creadas por ingenieros de sistemas y sólo la vende a un delincuente conocido, quien después de obtener la

[94] Código Civil de la República de Colombia, artículo 655, Santafe de Bogotá, Legis 2000.
[95] Corte Suprema de Justicia, sentencia del 22 de marzo de 1982, M.P. Dr. Alvaro Luna G., citada por Perez Pinzón, Alvaro, Delitos contra el patrimonio económico privado, Ediciones Forum Pacis, Bogotá 1992.Pág 45.

copia del software falso, lo instala en el computador alquilado y empieza a configurar el robo a quienes hacen transacciones bancarias por Internet.

Así, el cliente cree que ha ingresado a la página Web de determinada entidad bancaria, pero en realidad lo hizo a la página ficticia diseminada en la red del café Internet. El cliente, desprevenidamente aporta su clave personal y en ese mismo momento el ilícito toma cuerpo. El ahorrador cree que hizo la transacción pero ésta nunca se concretó, en cambio el ladrón quedó con su clave. Posteriormente, a través de un correo personal que adiciona al software falso, adquiere la información y vía Internet comienza a negociar con el dinero del incauto cliente, éste método se configura sin necesidad de intermediarios o de cómplices en las entidades financieras[96].

El hurto informático más común se da en el sistema financiero, ya que por su modernización es uno de los más automatizados en Latinoamérica, sin embargo, un caso para recordar fue el sonado Proceso 8.000, que involucró a la clase política colombiana, donde un funcionario de la Fiscalía ingresó a las computadoras de los fiscales regionales, copió las indagatorias y las vendió a un medio de información y obtuvo un lucro. Si fuera un sujeto procesal se le aplicaría las multas y penas del caso, no solo por haber violado la reserva del sumario sino por los demás delitos que estuvieran incursos, como la revelación del secreto oficial tipificado en el artículo 154 del C. P., o el Art 289 (Art. 194 nuevo C. P.) protección de documentos reservados, o el artículo 119 (espionaje), los cuales están en mora de modificarse porque se pueden cometer más fácilmente por vía automatizada. Además, el funcionario se convierte en infractor no de la ley común sino de la ley informática con la atenuante de que este tipo de ilícitos no se encuentran contemplados en sentido específico.

[96] Policía Nacional de Colombia, Delitos de mayor impacto social, Revista de la Policía Nacional de Colombia, Volumen 84, N0. 228, 1996

9. 1.3.2. Extorsión informática

Consiste en constreñir a alguien para obtener algún provecho fundamentalmente económico, valiéndose de medios como el secuestro o apoderamiento de soportes magnéticos en los que figure información valiosa, en una especie de chantaje.

El delito de extorsión tipificado en el reciente Código Penal, artículo 244 dice:
El que constriña a otro a hacer, tolerar u omitir alguna cosa, con el propósito de obtener provecho ilícito para sí o para un tercero, incurrirá en prisión de ocho (8) a quince (15) años.

Sujeto activo. Es indeterminado, ha de ser una persona natural. El sujeto activo tiene un ingrediente subjetivo dado por el provecho directo o de terceros que se espera obtener con la conducta. Más aún, no puede ser un servidor público porque se estaría hablando del delito de concusión.
Sujeto pasivo. Es el afectado económicamente por la conducta, debido a la actividad u omisión que le constriñe a ejecutar el extorsionador.
Objeto jurídico. Hay tres aspectos a tener en cuenta: con el comportamiento se afecta la autonomía personal convirtiéndose en un delito contra las garantías individuales, otro aspecto es el patrimonio económico que se va a ver afectado con la conducta, y un tercero se deriva del tipo de extorsión llamado chantaje, mediante el cual se pretende revelar aspectos íntimos de la vida de la persona atentando contra su intimidad y el derecho a la privacidad.
Objeto material. La conducta recae sobre el patrimonio, así, puede ser objeto material la entrega de información privada que posea un valor económicamente determinable.
Conducta. Está dada por el verbo rector constreñir que significa obligar, compeler o precisar por fuerza a otro a que haga o ejecute alguna acción, u obligar a alguien a hacer o no, mediante violencia material o moral.

Este es un delito correctamente tipificado, aplicado a las conductas de tipo informático, de manera tal que no genera problemas de tipicidad.

9.1.3.3. Estafa informática.

El delito de estafa se encuentra tipificado en el ordenamiento penal en el artículo 356 del C. P. (Art. 246 nuevo C. P.), y consiste en el provecho ilícito que se obtiene con daño patrimonial, empleando artificios o engaños idóneos para inducir a otro al error, pero como es estafa informática, sería valiéndose de la computadora o vulnerando sus seguridades.

> Artículo 246.-Estafa. El que obtenga provecho ilícito para sí o para un tercero, con perjuicio ajeno, induciendo o manteniendo a otro en error por medio de artificios o engaños, incurrirá en prisión de dos (2) a ocho (8) años y multa de cincuenta (50) a mil (1.000) salarios mínimos legales mensuales vigentes.

Sujeto activo. Es no calificado, hay indeterminación de la calidad del sujeto. Es toda persona natural, pues no admite estructuralmente responsabilidad de personas jurídicas.
Sujeto pasivo. Es igualmente indeterminado, puede ser una persona natural o jurídica.
Objeto jurídico. La estafa lesiona al bien jurídico patrimonio económico.
Objeto material. Está constituido por los bienes que, con la maniobra fraudulenta pasan a ser parte del patrimonio del agente o de un tercero.
Conducta. Está delimitada por un verbo rector, obtener, que significa lograr, alcanzar y adquirir. El artificio es una maquinación objetiva y exterior hecha exclusivamente para inducir o mantener en el error al sujeto pasivo de la conducta.

La existencia de la estafa es innegable en hechos donde el agente artificiosamente obtiene provecho mediante el uso de mecanismos que permiten la conexión autorizada por la computadora. Además en dichas conductas es más sutil el artificio entendiéndose que “toda estudiada y astuta transfiguración de la verdad”, se trata de una acción positiva, que la diferencia del engaño, como sería simular algo, o disimular, escondiendo lo que es como por ejemplo un estado de insolvencia. El engaño es un elemento fundamental de la estafa y se requiere que sea objetivado o se traduzca en hechos positivos.

9.1.3.4. Abuso de confianza informático.

Sucede cuando en calidad de bienes muebles, las computadoras y demás accesorios informáticos, son susceptibles de contratos de tenencia como el comodato o préstamo de uso, si el mero tenedor del bien informático dispone de él en la actualidad como si fuera el verdadero dueño, cometería el delito de abuso de confianza tipificado en los artículos 358 y 359 del actual C. P. (Arts 242 y 250 nuevo C. P.), a lo que el legislador está en mora de agravar esta conducta por tratarse de bienes informáticos. Así con un desalentador panorama por la mala previsión en técnica legislativa el mencionado delito reza así:

> Artículo 242: Abuso de confianza. El que se apropie en provecho suyo o de un tercero, de cosa mueble ajena, que se le haya confiado o entregado por un título no traslativo de dominio, incurrirá en prisión de (1) a cuatro (4) años y multa de (10) a doscientos (200) salarios mínimos legales mensuales vigentes.

Sujeto activo. Es no calificado, ha de ser una persona natural pues el tipo no permite la configuración de la responsabilidad penal de personas jurídicas[97].
Sujeto pasivo. Es igualmente indeterminado, se confunde con el perjudicado. Puede ser cualquier persona, natural o jurídica, que haya entregado un bien con un título no traslaticio de dominio.
Objeto jurídico. Definido en el tipo como perjuicio ajeno. Lesiona al bien jurídico patrimonio económico.
Objeto material. El objeto material es determinado por las cosas muebles. En este tipo la información no es parte de su objeto material.
Conducta. Está delimitada por el verbo rector apropiar, o sea sustraer, sacar de la esfera de dominio, el modelo está dado por acto de apoderamiento.
Elementos subjetivos y normativos. El elemento normativo está dado por la calidad del sujeto activo al decir que tiene la cosa por virtud de un título traslaticio de domino, noción que es parte de la legislación civil.

Las conductas cometidas con deslealtad, y que generan detrimento económico no pueden ser tipificadas como abuso de confianza debido al carácter único del objeto material de los delitos informáticos.

9.1.4. Delitos contra la fe pública.

9.1.4.1. Falsedad informática.

Conocida como falsedad vía computarizada, ya que a través de la computadora, se pueden contrahacer tarjetas de crédito, cheques, letras, títulos valores y todo tipo de documentos públicos o privados, alterar el sistema contable de una empresa, llevar

[97] MARQUEZ ESCOBAR, C. Op. Cit. Pág 186.

doble contabilidad a fin de evadir impuestos, delito que al tenor del artículo 43 de la Ley 222 de 1995 (reformatoria del C. de C.), donde la nueva tipicidad debió agravar la conducta dado que constituye una falsedad en documento privado[98].

Los artículos 218 a 228 del C. P. (Arts 273 a 296 del nuevo C. P.), contemplan los tipos de falsedad documentaria, y es claro que si se falsifica a través de computadora, se comete un delito contra la fe pública la cual debe ser sancionada, por lo cual debe construirse un nuevo tipo dentro de los delitos económicos pues no solo se está atentando contra la información sino contra la fe pública, asignando las penas y modalidades pertinentes.

Sujeto activo. El servidor público, ya que es el único con la aptitud de falsear ideológicamente el documento y el único facultado para la expedición. El tipo no se limita a particulares sino que agrava la punibilidad cuando el sujeto activo es un servidor público.
Sujeto pasivo. El Estado como único sujeto apto para conferir valor probatorio a cierto tipo de documentos.
Objeto jurídico. La fe pública es considerada como "el sentimiento colectivo de confianza que constituye un derecho de la sociedad y de los particulares en la veracidad, autenticidad e integridad de los signos de valor y de autenticación, de las formas escritas jurídicamente relevantes, como medios de prueba, y en la autenticidad de las personas, considerando todo ello, como elementos indispensables para el tráfico jurídico"[99]

[98] LEON MONCALEANO, W. Op Cit. Pág 204.
[99] ROMERO SOTO, Luis E., La falsedad documental, Bogotá, Temis, 1993, pág 48. La palabra "escrita" genera una ambigüedad que se puede presentar al incluir la noción de documento electrónico, el cual, según la noción común es un escrito paro en sentido estricto lo es solo en tanto que se utiliza un lenguaje llamado por la Ley 527 mensaje de datos, que reproducido a través del medio apropiado se entiende como escrito en el lenguaje que todos podemos entender.

Objeto material. En documento público, la falsedad ideológica genera que su objeto material sea la información que contenga dicho documento.
Conducta. Los verbos rectores son, consignar, callar y falsificar.
Elementos normativos. La facultad del servidor público para la expedición del documento determina si el delito es falsedad ideológica o una falsedad material agravada.

Entonces, si los artificios o engaños se ejecutan vía computadora para obtener un provecho económico, se puede catalogar como estafa informática lo cual excluiría las falsedades informáticas o falsedades comunes y corrientes, aunque según posición de la Sala de Casación Penal de la Corte Suprema de Justicia, solamente existe el delito de estafa, e insisten en que uno es el dolo y el objeto de tutela penal como en la fe pública y otro muy diferente el del patrimonio económico, lo cual es atentatorio del principio de la legalidad en tratándose de verdaderos delincuentes informáticos, pues las nuevas técnicas delictivas empleadas dejaron rezagadas las tipificaciones penales vigentes.

9.1.7. Delito de daño en obras o elementos de los servicios de comunicación.

9.1.7.1. Daño informático.

Dentro de los delitos contra el patrimonio económico, está el daño en cosa ajena, el cual se da, cuando una persona en forma deliberada atenta contra la computadora, los programas, la memoria, el disco duro o cualquiera de sus accesorios dañándolos o no permitiendo la ejecución, el cual se encuentra tipificado en el artículo 370 del Código Penal y artículo 265 Ley 599 de 2000, pues se inutilizó bien mueble con dolo, con deliberado propósito de causar daño, y la pena se encuentra consagrada

en el respectivo tipo penal, sin embargo es menester modificar expresamente la norma a fin de señalar como agravante el haber atentado contra bien informático y no poner a cavilar a los investigadores y falladores sobre si "el objeto de interés científico" es la computadora o la red. Aunque la solución más acertada sería crear un nuevo tipo penal de daño en bien informático que no solamente comprenda el daño físico a la computadora sino todas las consecuencias que conlleva y que tienen que ver con el *software* que es lo que constituye el verdadero daño informático, pues con este actuar el delincuente está atentando contra la verdad, contra la fe pública y ahí es donde se debe establecer la "falsedad informática de documentos públicos o privados por supresión o destrucción"[100].

Otro tipo de daño referente al *software* se da cuando se le ha inoculado virus, causando daños a la computadora fundamentalmente a los comando internos o interactivos, a fin de evitar que se reproduzca o copie un programa, delito contemplado en la Ley de Derechos de Autor, artículo 270 numeral 3 Título VIII del Nuevo Código Penal, donde se trata como un ataque al patrimonio económico cuando en realidad la propia norma indica que se está atentando contra el derecho moral de autor.

Sujeto activo. Es indeterminado. "No hay lugar a responsabilidad de personas jurídicas, por lo tanto el agente del delito siempre será una persona natural.
Sujeto pasivo. Es aquel que sufre el daño patrimonial por la acción delictiva.
Objeto jurídico. Es el patrimonio económico. No se ve afectado ningún otro bien jurídico de modo que el delito es mono-ofensivo.
Objeto material. Son los bienes corporales sean muebles o inmuebles. El objeto debe ser ajeno para que incurra en conducta delictiva.

[100] LEON MONCALEANO, William Fernando, Op. Cit. Pág 191.

Conducta. Está definida por cuatro verbos rectores: destruir, inutilizar, desaparecer y dañar, lo que implica arruinar, deshacer, hacer inoperante una cosa, echarlo a perder[101].

El comportamiento, en cuanto a la información se hace atípico, pues no existe norma que condene el daño de información, lo cual es desalentador si se tiene en cuenta que la tecnología y los procesos de automatización de información desempeñan un papel fundamental en lo económico y en lo político. Desprotección penal que desalienta cualquier actividad investigativa.

9.1.6. Delitos contra la libertad, integridad y formación sexual.

9.1.6.1. La corrupción de menores vía informática.

El Código Penal en su artículo 205 en el título de los "Delitos contra la Libertad Sexual y la Dignidad Humana", la corrupción de menores, normatividad que fue subrogada por la Ley 360 de 1997 en su artículo 7º donde aumentó las penas para los delitos denominados sexuales y que en el nuevo Código Penal se tipificó en la parte final del artículo 209 como Acto Sexual con menor de 14 años, el 218 como Pornografía con menores, normatividad que se relaciona con los artículos 217 (Estímulo a la prostitución de menores), y el 219 (Turismo sexual con menores), conductas atentatorias de la Libertad, Integridad y Formación Sexual.

> Artículo 212. Pornografía con menores. El que fotografíe, filme, venda, compre, exhiba o de cualquier manera comercialice material pornográfico en el que participen menores de edad, incurrirá en prisión de tres (3) a ocho (8) años y

[101] MARQUEZ ESCOBAR, C. Op cit. Pág 180

multa de cien (100) a mil (1.000) salarios mínimos legales mensuales vigentes[102].

Sujeto activo. No es calificado, por lo tanto es indeterminado, además no tiene ningún elemento subjetivo o normativo que califique la actividad del sujeto activo.
Sujeto pasivo. Es calificado por la edad, el sujeto sobre el cual recae el comportamiento son los menores de 18 años.
Objeto jurídico. El bien jurídico tutelado está destinado a proteger la libertad sexual como "el derecho de toda persona para disponer de su cuerpo, en lo erótico, como a bien tenga"[103].
Objeto material. Es el material en el que se transmite la expresión pornográfica, lo cual es de por sí ambiguo pues depende de la decisión del juez quien en último determina que es o no pornográfico.
Conducta. Los verbos rectores son fotografiar, filmar, vender, comprar, exhibir o comercializar.

Es incontrovertible que hoy en día, una de las formas de inducir a la corrupción es por medio de la computadora, el sujeto corruptor puede inducir a los niños a prácticas sexuales a través de imágenes y videos, casos en los que responderá por corrupción de menores, pero es lamentable que la reciente ley no se haya referido a estos nuevos sistemas aptos para la corrupción y la elaboración de la pornografía, con grabaciones de actos homosexuales o heterosexuales, con escenas verdaderamente inmorales, y haya aumentado las penas por tratarse de corrupción de menores por medio de la informática, pues sería ilógico aplicar las sanciones simplemente de pornografía contempladas en el Código Nacional de Policía que de por si son multas insignificantes.

[102] CODIGO PENAL de 2000, Santafe de Bogotá, Legis, 2000.
[103] BARRERA DOMINGUEZ, Humberto, Delitos contra la vida e integridad personal, Bogotá, Jurídica Radar, 1985. pág 53.

En otros países la situación es diferente, por ejemplo, un profesor de la Facultad de Informática de la Universidad de Granada se enfrenta a un total de 48 años de prisión acusado de contactar a través de internet a seis menores de distintos puntos del país, a los que supuestamente conoció haciéndose pasar por una niña, y a los que recargaba el móvil a cambio de que se desnudaran frente a la pantalla, para captar su imagen desde su 'webcam'. El procesado, negó los hechos, y al parecer, amenazaba a los niños, con edades de entre 10 y 12 años, si contaban lo ocurrido a sus padres.

El profesor reconoció haber entrado en contacto con los seis menores, y aseguró que lo hizo a través de una página de juegos 'on-line' y que sus conversaciones a través del correo electrónico o 'Messenger' tenían el objetivo de "sincronizarse" con los menores, para jugar a la vez en esa web. En la inspección a su ordenador, se encontraron vídeos de contenido pedófilo, fotografías y relatos en inglés de pornografía infantil. El procesado se conectaba al 'Messenger' para hablar con los niños, frente a los que llegó a desnudarse, a través de su 'webcam', y a los que instó también a quitarse la ropa, algo que sólo consiguió en uno de los casos, por las amenazas que le estaba profiriendo, asegurando ser policía.

En nuestro país la Ley 360 en sus artículos 12 y 13 denominados “Estímulo la prostitución de menores y pornografía con menores” en donde se debe considerar que el bienestar de los niños es de imperativo interés del Estado, teniendo en cuenta que si los niños poseen nacientes y elementales deseos sexuales, ellos no están plenamente formados, carecen de experiencia y madurez, son vulnerables a la exposición de materiales sexuales y a la explotación de predadores con deseos sexuales anormales, por lo que se hace necesaria una verdadera legislación preventiva y de vigilancia en la materia y las sanciones penales del caso aunque con un nuevo tipo que especifique los problemas concernientes a la corrupción de menores sistematizada. Ya que ésta nueva Ley se ha quedado corta y rezagada,

pues en su descripción típica sanciona la compraventa y exhibición de pornografía infantil y no las filmaciones o fotografías de los niños realizando dichas prácticas.

Sobre éste fenómeno informático pornográfico, se han pronunciado autores como PATRICIA CHOCK y LEE TIEN de la universidad de California: "En el caso de los computadores, los peligros son supuestamente mayores que los de otros medios, creemos que los niños tiene una afinidad por nuevas tecnologías, tales como los computadores. La habilidad de los niños de acomodarse dentro de las comunicaciones de los computadores *(hacking)* es bien conocida. Ellos ven las redes de información como un juego, los computadores son extremadamente accesibles a los niños. Los niños están siendo entrenados para usar computadores en la escuela…más y más padres están comprando computadores domésticos para sus hijos[104].

Así, el medio visual es considerado como potencialmente nocivo y la computadora proporciona la posibilidad de manejar gráficas digitalizadas electrónicamente, estas pueden ser preservadas y reproducidas más fácilmente que las fotografías convencionales. El niño que ha posado para una cámara crece sabiendo que la grabación es susceptible de circulación masiva creándole una serie de traumas y conflictos.

Hay que tener en cuenta que las comunicaciones por computador son relativamente anónimas para ambas partes, así el niño puede pasar como un adulto en una red de computador que a través de la línea telefónica. Este relativo anonimato permite al pedófilo establecer contacto y desarrollar una relación sin necesidad de cambiar nombres u otra información, éste sentido de privacidad y del secreto satisfacen las

[104] CHOCK Patricia. El uso de los computadores en la explotación sexual de los niños y en la pornografía infantil.

necesidades de individuos que están interesados en traficar, negociar y coleccionar pornografía infantil y obscenidad…"[105]

9.1.7. Delitos contra la seguridad del estado.

9.1.7.1. Espionaje informático.

Este delito contra la seguridad del Estado se encuentra tipificado en el artículo 463 así: El que indebidamente obtenga, emplee o revele secreto político, económico o militar relacionado con la seguridad del Estado, incurrirá en prisión de cuatro (4) a doce (12) años.

Sujeto activo. El sujeto activo es no calificado.
Sujeto pasivo. Es el Estado.
Objeto jurídico. Es la seguridad y existencia del Estado.
Objeto material. Es la información que tiene el carácter de ser secreta y que por su confidencialidad puede menoscabar la seguridad del Estado.
Conducta. Los verbos rectores son: obtener, emplear y revelar. Consiste en la ejecución de actos que obtengan, revelen y empleen secretos de tipo político, económico y militar.
Elemento normativo. Está dado por el vocablo "indebidamente" lo que significa que aquel que obtenga la información no tiene derecho a emplearla o revelarla por existir la prohibición legal para hacerlo.
El *modus operandi* en nuestro país no es de gran trascendencia debido a la retrasada tecnología del sistema gubernativo[106].

[105] LEE TIEN. La sexualidad infantil y las nuevas tecnologías de la información. Universidad de California. Traducción del profesor JOSE LUIS ARAMBURO RESTREPO Facultad de Derecho. Universidad Nacional. Bogotá. 1995
[106] MARQUEZ ESCOBAR, C. Op cit. Pág 267.

9.1.8. Otros delitos.

9.1.8.1. Delito Phishing[107]

Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. El término *phishing* proviene de la palabra inglesa "*fishing*" (pesca), haciendo alusión al intento de hacer que los usuarios "piquen en el anzuelo". A quien lo practica se le llama *phisher*. La primera mención del término *phishing* data de enero de 1996.

Phishing en MSN Messenger

Dos de los ejemplos más recientes son las páginas **quienteadmite** y **noadmitido** destinadas a robar el nombre y contraseña de los usuarios de MSN a cambio de mostrarle a los visitantes que las utilicen, quien los ha borrado de su lista de contactos. Esta técnica consiste en pedirle al usuario final su usuario o correo electrónico y luego la contraseña, datos que son enviados luego a la base de datos del autor de la página, y así almacenar la información para poder acceder a dichas cuentas.

Los intentos más recientes de phishing han tomado como objetivo a clientes de bancos y servicios de pago en línea. Estudios recientes muestran que los

[107] http://es.wikipedia.org/wiki/pishing=cite-note-1.

phishers en un principio son capaces de establecer con qué banco tiene relación la posible víctima, y de ese modo enviarle un e-mail, falseado apropiadamente.

Esta variante hacia objetivos específicos en el phishing se ha denominado *spear phishing* (literalmente *pesca con arpón*). Los sitios de Internet con fines sociales también se han convertido en objetivos para los phishers, dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad. Algunos experimentos han otorgado una tasa de éxito de un 90% en ataques phishing en redes sociales. A finales de 2006 un gusano informático se apropió de algunas páginas del sitio web MySpace logrando redireccionar los enlaces de modo que apuntaran a una página web diseñada para robar información de ingreso de los usuarios.

Técnicas de phishing

La mayoría de los métodos de phishing utilizan alguna forma técnica de engaño en el diseño para mostrar que un enlace en un correo electrónico parezca una copia de la organización por la cual se hace pasar el impostor. URLs mal escritas o el uso de subdominios son trucos comúnmente usados por phishers, como el ejemplo en esta URL, http://www.nombredetubanco.com.ejemplo.com/. Otro ejemplo para disfrazar enlaces es el de utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar el nombre de usuario y contraseña (contrario a los estándares). Por ejemplo, el enlace http://www.google.com@members.tripod.com/ puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando realmente el enlace envía al navegador a la página de members.tripod.com (y al intentar entrar con el nombre de usuario de www.google.com, si no existe tal usuario, la página abrirá normalmente). Este método ha sido erradicado desde entonces en los navegadores de Mozilla e

Internet Explorer. Otros intentos de phishing utilizan comandos en JavaScripts para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL ilegítima[108].

En otro método popular de phishing, el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. En este método de ataque (conocido como Cross Site Scripting) los usuarios reciben un mensaje diciendo que tienen que "verificar" sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

Lavado de dinero producto del phishing

Actualmente empresas ficticias intentan reclutar teletrabajadores por medio de e-mails, chats, irc y otros medios, ofreciéndoles no sólo trabajar desde casa sino también otros jugosos beneficios. Aquellas personas que aceptan la oferta se convierten automáticamente en *víctimas* que incurren en un grave delito sin saberlo: el blanqueo de dinero obtenido a través del acto fraudulento de phishing.

Para que una persona pueda darse de alta con esta clase de *empresas* debe llenar un formulario en el cual indicará, entre otros datos, su número de cuenta bancaria. Esto tiene la finalidad de ingresar en la cuenta del *trabajador-víctima* el

[108] http://es.wikipedia.org/wiki/pishing=cite-note2

dinero procedente de estafas bancarias realizadas por el método de *phishing*. Una vez *contratada*, la víctima se convierte automáticamente en lo que se conoce vulgarmente como *mulero*.

Con cada acto fraudulento de *phishing* la víctima recibe el cuantioso ingreso en su cuenta bancaria y la empresa le notifica del hecho. Una vez recibido este ingreso, la víctima se quedará un porcentaje del dinero total, pudiendo rondar el 10%-20%, como comisión de trabajo y el resto lo reenviará a través de sistemas de envío de dinero a cuentas indicadas por la *seudo-empresa*.

Fases[109]

- En la primera fase, la red de estafadores se nutre de usuarios de chat, foros o correos electrónicos, a través de mensajes de ofertas de empleo con una gran rentabilidad o disposición de dinero (hoax o scam). En el caso de que caigan en la trampa, los presuntos intermediarios de la estafa, deben llenar campos, tales como: Datos personales y número de cuenta bancaria.
- Se comete el phishing, ya sea el envío global de millones de correos electrónicos bajo la apariencia de entidades bancarias, solicitando las claves de la cuenta bancaria (PHISHING) o con ataques específicos.
- El tercer paso consiste en que los estafadores comienzan a retirar sumas importantes de dinero, las cuales son transmitidas a las cuentas de los intermediarios (muleros).
- Los intermediarios realizan el traspaso a las cuentas de los estafadores, llevándose éstos las cantidades de dinero y aquéllos —los intermediarios— el porcentaje de la comisión.

[109] http://es.wikipedia.org/wiki/pishing=cite-note3

Daños causados por el phishing

Los daños causados por el phishing oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales. Este tipo de robo de identidad se está haciendo cada vez más popular por la facilidad con que personas confiadas normalmente revelan información personal a los phishers, incluyendo números de tarjetas de crédito y números de seguridad social. Una vez esta información es adquirida, los phishers pueden usar datos personales para crear cuentas falsas utilizando el nombre de la víctima, gastar el crédito de la víctima, o incluso impedir a las víctimas acceder a sus propias cuentas.

Se estima que entre mayo de 2004 y mayo de 2005, aproximadamente 1,2 millones de usuarios de computadoras en los Estados Unidos tuvieron pérdidas a causa del phishing, lo que suma a aproximadamente $929 millones de dólares estadounidenses. Los negocios en los Estados Unidos perdieron cerca de 2000 millones de dólares al año mientras sus clientes eran víctimas. El Reino Unido también sufrió el alto incremento en la práctica del phishing. En marzo del 2005, la cantidad de dinero reportado que perdió el Reino Unido a causa de esta práctica fue de aproximadamente £12 millones de libras esterlinas[110.]

Respuestas legislativas y judiciales

El 26 de enero de 2004, la FTC (*Federal Trade Commission*, "Comisión Federal de Comercio") de Estados Unidos llevó a juicio el primer caso contra un *phisher* sospechoso. El acusado, un adolescente de California, supuestamente creó y utilizó una página web con un diseño que aparentaba ser la página de América Online para poder robar números de tarjetas de crédito. Tanto Europa como Brasil siguieron la práctica de los Estados Unidos, rastreando y arrestando a

[110] http://es.wikipedia.org/wiki/pishing=cite-note4

presuntos *phishers*. A finales de marzo de 2005, un hombre estonio de 24 años fue arrestado utilizando una *backdoor*, a partir de que las víctimas visitaron su sitio web falso, en el que incluía un *keylogger* que le permitía monitorear lo que los usuarios tecleaban. Del mismo modo, las autoridades arrestaron al denominado phisher kingpin, Valdir Paulo de Almeida, líder de una de las más grandes redes de phishing que en dos años había robado entre $18 a $37 millones de dólares estadounidenses. En los Estados Unidos, el senador Patrick Leahy introdujo el *Acta Anti-Phishing de 2005* el 1 de marzo de 2005. Esta ley federal de anti-*phishing* establecía que aquellos criminales que crearan páginas web falsas o enviaran spam a cuentas de e-mail con la intención de estafar a los usuarios podrían recibir una multa de hasta $250,000 USD y penas de cárcel por un término de hasta cinco años.[111]

La compañía Microsoft también se ha unido al esfuerzo de combatir el *phishing*. El 31 de marzo del 2005, Microsoft llevó a la Corte del Distrito de Washington 117 pleitos federales. En algunos de ellos se acusó al denominado *phisher* "John Doe" por utilizar varios métodos para obtener contraseñas e información confidencial. Microsoft espera desenmascarar con estos casos a varios operadores de phishing de gran envergadura. En marzo del 2005 también se consideró la asociación entre Microsoft y el gobierno de Australia para educar sobre mejoras a la ley que permitirían combatir varios crímenes cibernéticos, incluyendo el phishing.

Una vez más, Abogados Portaley, despacho especializado en delitos informáticos, ha conseguido el sobreseimiento provisional y archivo de la causa en un procedimiento penal seguido por estafa informática llevada a cabo a través del conocido método Phishing.

[111] http://es.wikipedia.org/wiki/pishing=cite-note5

El Juzgado de Instrucción nº 7 de Parla (Madrid) en el procedimiento seguido con D.P. 1084/09, ha dictado Auto acordando el sobreseimiento provisional y archivo de la causa al entender que la imputada (mulera) actuó de buena fe en los hechos.

El Auto fundamenta jurídicamente su fallo de la siguiente manera:

> A la vista de toda la prueba practicada en el procedimiento, resulta acreditado que la imputada actuó de buena fe, ya que acredita documentalmente la oferta de trabajo que recibió, el contrato que firmó, los correos electrónicos que recibió y envió a los responsables de la empresa ficticia. Además, consta que al enterarse de lo que ocurría, ya que fue avisada por su banco, se puso en contacto con el director de la sucursal bancaria y ordenó la devolución de las transferencias que todavía estaban en su poder, por todo ello, y entendiendo que no tuvo conocimiento de las irregularidad de las operaciones que realizaba, de conformidad con el principio de presunción de inocencia y de in dubio pro reo, procede acordar el sobreseimiento provisional y archivo de las actuaciones.

9.1.8.2. Delito Spoofing[112]

En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Existen diferentes tipos dependiendo de la tecnología a la que nos refiramos, los cuales se describirán más adelante, como el IP spoofing (quizás el más conocido), ARP spoofing, DNS spoofing, Web spoofing o e-mail spoofing, aunque en general se puede englobar dentro de spoofing cualquier tecnología de red susceptible de sufrir suplantaciones de identidad.

[112] http://es.wikipedia.org/wiki/pishing=cite-note6

Tipos de Spoofing

- **IP Spoofing**: suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Hay que tener en cuenta que las respuestas del host que reciba los paquetes alterados irán dirigidas a la IP falsificada. Por ejemplo si enviamos un ping (paquete icmp "echo request") spoofeado, la respuesta será recibida por el host al que pertenece la IP legalmente. Este tipo de spoofing unido al uso de peticiones broadcast a diferentes redes es usado en un tipo de ataque de flood conocido como ataque Smurf.

- **ARP Spoofing**: suplantación de identidad por falsificación de tabla ARP. Se trata de la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. Explicándolo de una manera más sencilla: El protocolo Ethernet trabaja mediante direcciones MAC, no mediante direcciones IP. ARP es el protocolo encargado de traducir direcciones IP a direcciones MAC para que la comunicación pueda establecerse; para ello cuando un host quiere comunicarse con una IP navegador que muestre en todo momento la IP del servidor visitado, si la IP nunca cambia al visitar diferentes páginas WEB significará que probablemente estemos sufriendo este tipo de ataque.

- **Mail Spoofing**: Suplantación en correo electrónico de la dirección e-mail de otras personas o entidades. Esta técnica es usada con asiduidad para el envío de e-mails hoax como suplemento perfecto para el uso de phising y para SPAM, es tan sencilla como el uso de un servidor SMTP configurado para tal fin. Para protegerse se debería comprobar la IP del remitente (para averiguar si realmente esa IP pertenece a la entidad que indica en el mensaje) y la dirección del servidor SMTP utilizado. Otra técnica de protección es el uso de firmas digitales[113].

9.1.8.3. Delito Hijacking

Hijacking significa "secuestro" en inglés y en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñarse o robar algo (generalmente información) por parte de un atacante. Es por tanto un concepto muy abierto y que puede aplicarse a varios ámbitos, de esta manera podemos encontrarnos con el secuestro de conexiones de red, sesiones de terminal, emite una trama ARP-Request a la dirección de Broadcast pidiendo la MAC del host poseedor la IP con la que desea comunicarse. El ordenador con la IP solicitada responde con un ARP-Reply indicando su MAC. Los Switches y los hosts guardan una tabla local con la relación IP-MAC llamada "tabla ARP". Dicha tabla ARP puede ser falseada por un ordenador atacante que emita tramas ARP-REPLY indicando su MAC como destino válido para una IP específica, como por ejemplo la de un router, de esta manera la información dirigida al router pasaría por el ordenador atacante quien podrá sniffar dicha información y redirigirla si así lo desea.

[113] http://es.wikipedia.org/wiki/pishing=cite-note8

Web Spoofing: Suplantación de una página web real (no confundir con phising). Enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información de dicha víctima (páginas WEB vistas, información de formularios, contraseñas etc.). La página WEB falsa actúa a modo de proxy solicitando la información requerida por la víctima a cada servidor original y saltándose incluso la protección SSL. El atacante puede modificar cualquier información desde y hacia cualquier servidor que la víctima visite. La víctima puede abrir la página web falsa mediante cualquier tipo de engaño, incluso abriendo un simple LINK. El WEB SPOOFING es difícilmente detectable, quizá la mejor medida es algún plugin del servicios, modems y un largo etcétera en cuanto a servicios informáticos se refiere.

Algunos ejemplos de Hijacking

- **IP hijakers**: secuestro de una conexión TCP/IP por ejemplo durante una sesión Telnet permitiendo a un atacante inyectar comandos o realizar un DoS durante dicha sesión.
- **Page hijacking**: secuestro de página web. Hace referencia a las modificaciones que un atacante realiza sobre una página web, normalmente haciendo uso de algún bug de seguridad del servidor o de programación del sitio web, también es conocido como defacement o desfiguración.
- **Home Page Browser hijacking**: secuestro de la página de inicio del navegador. Esto sucede cuando la página de inicio, en la que navegamos es cambiada por otra a interés del secuestrador. Generalmente son páginas en las que nos invita a usar los servicios de la página para que nuestro equipo esté seguro y funcione correctamente. No cabe decir que es a cambio de un pago y que el origen del error y mal funcionamiento del equipo es debido a nuestro secuestrador

- **Modem hijacking**: secuestro del Modem. Esta expresión es en ocasiones utilizada para referirse a la estafa de los famosos dialers que tanta guerra dieron en su día (antes del auge del ADSL) y que configuran sin el consentimiento del usuario nuevas conexiones a números de cobro extraordinario.
- **Thread hijacking**: secuestro de un "tema" dentro de un foro de discusión de internet. Este término hace referencia a la situación que ocurre cuando dentro de un tema de discusión en un foro alguien intenta dirigir el hilo de la conversación hacia asuntos que no tienen nada que ver con el tema inicial. Esto puede realizarse de manera intencionada para irritar al autor del tema o bien producirse de manera natural y no intencionada generalmente por usuarios sin mucho conocimiento en el asunto a tratar o que desconocen la dinámica de comportamiento de los foros.

Algunos de los primeros programas infecciosos, incluyendo el primer gusano de Internet y algunos virus de MS-DOS, fueron elaborados como experimentos, bromas o simplemente como algo molesto, no para causar graves daños en las computadoras. En algunos casos el programador no se daba cuenta de cuánto daño podía hacer su creación. Algunos jóvenes que estaban aprendiendo sobre los virus los crearon con el único propósito de probar que podían hacerlo o simplemente para ver con qué velocidad se propagaban. Incluso en 1999, un virus tan extendido como Melissa parecía haber sido elaborado como una travesura.

Por otra parte, un gusano es un programa que se transmite a sí mismo, explotando vulnerabilidades, en una red de computadoras para infectar otros equipos. El principal objetivo es infectar a la mayor cantidad de usuarios posible, también puede contener instrucciones dañinas al igual que los virus.

Un virus necesita de la intervención del usuario para propagarse mientras que un gusano se propaga automáticamente. Teniendo en cuenta esta distinción, las infecciones transmitidas por Email o documentos de Microsoft Word, que dependen de su apertura por parte del destinatario para infectar su sistema, deberían ser clasificadas más como virus que como gusanos. Algunos periodistas y vendedores parecen no comprender esta diferencia y usan los términos indistintamente.

9.1.8.4. ROOTKITS

Las técnicas conocidas como rootkits modifican el sistema operativo de una computadora para permitir que el malware permanezca oculto al usuario. Por ejemplo, los rootkits evitan que un proceso malicioso sea visible en la lista de procesos del sistema o que sus ficheros sean visibles en el explorador de archivos. Este tipo de modificaciones consiguen ocultar cualquier indicio de que el ordenador esta infectado por un malware. Originalmente, un rootkit era un conjunto de herramientas instaladas por un atacante en un sistema Unix donde el atacante había obtenido acceso de administrador (acceso root). Actualmente, el término es usado generalmente para referirse a la ocultación de rutinas en un programa malicioso.

Algunos programas maliciosos también contienen rutinas para evitar ser borrados, no sólo para ocultarse. Un ejemplo de este comportamiento puede ser:

> *"Existen dos procesos-fantasmas corriendo al mismo tiempo. Cada proceso-fantasma debe detectar que el otro ha sido terminado y debe iniciar una nueva instancia de este en cuestión de milisegundos. La única manera de eliminar ambos procesos-fantasma es eliminarlos*

simultáneamente, cosa muy difícil de realizar, o provocar un error el sistema deliberadamente." [114]

Uno de los rootkits más famosos fue el que la empresa Sony incluyo dentro de la protección anticopia de algunos CDs de música.

9.1.8.5. Puertas Traseras o Backdoors

Una puerta trasera o backdoor es un método para eludir los procedimientos normales de autenticación a la hora de conectarse a una computadora. Una vez que el sistema ha sido comprometido (por uno de los anteriores métodos o de alguna otra forma) una puerta trasera puede ser instalada para permitir un acceso remoto más fácil en el futuro. Las puertas traseras también pueden ser instaladas previamente al software malicioso para permitir la entrada de los atacantes.

Los crackers suelen usar puertas traseras para asegurar el acceso remoto a una computadora, intentado permanecer ocultos ante una posible inspección. Para instalar puertas traseras los crackers pueden usar troyanos, gusanos u otros métodos.

La idea de que los fabricantes de ordenadores preinstalan puertas traseras en sus sistemas para facilitar soporte técnico a los clientes ha sido sugerida a menudo pero no ha llegado a ser comprobada nunca de forma fiable.

[114] http://es.wikipedia.org/wiki/pishing=cite-note11

10. ESTUDIO DE CASOS.

Nicolás Castro fue capturado por la Dijín, y la Fiscalía le imputó cargos ante un juez, quien ordenó recluirlo en la cárcel La Picota. Su captura generó un debate sobre el castigo para quienes hacen amenazas por Internet[115].

El abogado Wilson Rivera, defensor de Nicolás Castro, le dijo ayer a EL TIEMPO que desde hace cuatro meses su cliente se había presentado ante las autoridades y había explicado que todo se trataba de una broma. "Fue con los computadores a la Dijín y dijo que para él era una recocha (broma). Las autoridades sabían todo y tenían identificada su casa y dónde estudiaba", explicó el abogado Rivera.

Agregó el defensor de Nicolás Castro, creador del grupo "Me comprometo a matar a Jerónimo Alberto Uribe", que su cliente expresó su opinión por medio de monólogo. "No constituye ningún delito. Es un tema de libertad de opinión, en un capítulo que él ya cerró", dijo.

10.1. Debate sobre amenazas por Internet

El tema desató un debate por las amenazas que circulan en las llamadas redes sociales de la web y los resultados en las investigaciones por esos casos. Una de las que se pronunció fue la senadora Piedad Córdoba, quien afirmó que a pesar de que ha sido amenazada en por lo menos 20 páginas creadas en las redes sociales, aún no hay resultados en las investigaciones.

[115] http:// www. eltiempo.com/Colombia/justicia/

"El grupo (de amenaza de muerte) al hijo de Uribe estuvo al aire 10 horas y aún así hay presos, los que me querían matar estuvieron al aire por meses (...) yo tengo los registros, uno busca un sicario para asesinarme, otro hace colecta para quemarme y otro una bomba", dijo ayer la parlamentaria a través de su cuenta de en la red social conocida como Twitter.

El DAS investigó en el 2009, 28 casos de amenazas en internet (dos de ellos contra Gustavo Petro) y este año, otros 18. Las amenazas de este año llegaron contra personajes como Petro, Carlos Gaviria, la Dirección del Polo Democrático, la Dirección de Derechos Humanos del Ministerio del Interior, la Universidad del Valle, el Fondo Nacional del Ahorro, entre otras. En varios casos se llegó a ubicar el sitio donde escribieron las amenazas: uno de ellos, por ejemplo, resultó ser un café internet cercano a una sede del Polo en Bogotá. Pero el caso no fue judicializado por los afectados.

A su vez, la Dijín reveló que realiza 23 investigaciones de amenazas por la red a diferentes personas, similares al caso de Nicolás Castro, el universitario señalado de ser el creador de la página de Facebook contra Jerónimo Uribe, hijo del Presidente. El general Gilberto Ramírez, comandante de la Dijín, indicó que el rastreo realizado a los computadores de Castro reveló que había hecho 1.400 consultas en Internet sobre la familia presidencial, y que era asiduo visitante de páginas de grupos como las Farc y Alqaeda.

"A través del acceso que tiene como miembro de estas páginas que apoyan el terrorismo internacional, que apoyan a las Farc para ser más exactos, podemos decir que él accedió a estas páginas con el fin de obtener información privilegiada sobre estos temas", afirmó el general Ramírez. Frente al tema, una fuente de la Fiscalía explicó que así Jerónimo Uribe retire los cargos, el caso debe seguir hasta que haya una decisión de un juez.

11. CONSIDERACIONES DE LA CORTE CONSTITUCIONAL

Algunos conceptos emitidos por la Honorable Corte Constitucional, Corte Suprema de Justicia y el Consejo de Estado, sobre la Internet, el comercio electrónico y los delitos informáticos.

SENTENCIA T-729 de 2002 de la Corte Constitucional.

Dentro del proceso de revisión del fallo proferido por la Sala Laboral del Tribunal Superior de Distrito judicial de Bogotá en única instancia, dentro del expediente de tutela T-467.

Hechos. El departamento Administrativo de Catastro del Distrito Capital, a partir del año 2001, dispuso en la Internet una página virtual que incorpora una base de datos sobre la información catastral de Bogotá, solamente digitando el número de identificación de cualquier persona es posible obtener información detallada del predio tanto jurídica como económica.

Así mismo, la Superintendencia Nacional de Salud dispuso en la Internet una página virtual que incorpora una base de datos con información relativa a la afiliación al régimen de seguridad social en salud, con la cual, mediante la digitación del número del documento de identificación de cualquier persona, es posible acceder a información relativa al afiliado.

El tutelante aduce que si cualquier persona puede acceder a los datos personales se están desconociendo sus derechos fundamentales a la

autodeterminación informática o a la intimidad. A lo cual el Tribunal concluye que: “con la existencia de la información en dichas páginas de la Internet, no se pone en peligro la integridad física que aduce el tutelante, cuando solamente se arrojan datos que corresponden a la generalidad de la información de los usuarios.

Sin embargo, la Corte considera indispensable que se establezcan normas respecto a:

- Adoptar mecanismos de seguridad adecuados, que permitan la salvaguardia de la información contenida en la base de datos.
- Normas que establezcan sanciones y regímenes especiales de responsabilidad para las entidades administradoras de base de datos y para los usuarios de la información.
- Normas dirigidas a desestimular y sancionar prácticas indebidas en ejercicio del poder informático: cruce de datos, divulgación indiscriminada, bases de datos secretas, y otros.
- Normas que regulen los procesos internos de depuración y actualización de datos personales, así como los de las solicitudes de rectificación, adición y supresión de los mismos.

Igualmente, a fin de establecer el equilibrio entre los derechos a la información y a la autodeterminación informática, es importante que se tenga en cuenta, tanto el principio de la responsabilidad compartida donde quien solicita la información, y el que la suministra, tengan en cuenta la existencia de un interés protegido del titular del dato, como el principio de cargas mutuas, donde a mayor información solicitada por un tercero, mayor detalle sobre su identidad y sobre la finalidad de la información.

Respecto a los datos personales dispuestos en la página de Internet de Catastro, la Corte considera que su conducta no se ajusta al principio de libertad en los procesos de administración de datos, que además dicha entidad desconoce de manera indirecta el principio de finalidad en cuanto que permite el acceso indiscriminado a la información personal, y que esta información aunque sea precaria constituye un riesgo cierto que debe ser evitado ante la posible elaboración de perfiles virtuales, lo que conduce a analizar el alcance al principio de individualidad.

En cuanto a los datos dispuestos en la página de Internet por la Superintendencia Nacional de Salud, la Corte considera que se está vulnerando el derecho fundamental a la Autodeterminación informática, ya que se trata de la publicación de datos personales catalogados como información semi-privada, a la cual se puede acceder con el sencillo requisito de digitar el numero de identificación, desconociendo los principios constitucionales de libertad, finalidad, circulación restringida e individualidad propios de la administración de datos personales.

Vemos como la Corte Constitucional amplía su visión hacia la modernización del Estado proponiendo la creación de unos parámetros que permitan la salvaguardia de los derechos constitucionales fundamentales, así como la reglamentación del uso del poder informático que se ha venido desarrollando con la Internet, el cual está caracterizado por el anonimato y la carencia de controles aumentando los riesgos de infracción efectiva no solo en el derecho de autodeterminación informática sino en los demás derechos fundamentales.

Sentencia C- 1147 /01 de la Corte Constitucional

Magistrado Ponente: Manuel José Cepeda Espinosa. Octubre 31 de 2001. Registro Mercantil y Comercio Electrónico.

En ejercicio de la acción pública de inconstitucionalidad, un ciudadano presentó una demanda contra el artículo 91 de la Ley 633 de 2000 el cual establece: *"Todas las páginas web y los sitios de internet de origen colombiano que operan en el internet y cuya actividad económica sea de carácter comercial, financiera o de prestación de servicios, deberán inscribirse en el registro mercantil y suministrar a la Dirección de Impuestos y Aduanas Nacionales DIAN, la información de transacciones económicas en los términos en que esta entidad lo requiera"*

En opinión del actor, dicha disposición vulnera los artículos 4, 15, 101, 158 y 363 de la Constitución Política, pues el legislador no adelantó criterio legal para delimitar adecuadamente el ámbito de la disposición, creando una situación de incertidumbre sobre si su actividad cae o no bajo el imperio de esta Ley. En referencia a "de origen colombiano", pueden ser las páginas que contienen la sigla *´co´*, o las páginas con nombre terminado en *´com´* que hayan sido abiertas por un nacional colombiano y sean operadas desde el país o desde el exterior por el mismo.

Adicionalmente, el artículo en cuestión no señala los términos de esta facultad sino que traslada su responsabilidad constitucional en forma indebida, permitiendo a la autoridad que debería ser objeto de control, fijar el límite de su propia introducción en la esfera privada y suministrar a la Dirección de Impuestos y Aduanas la información de transacciones económicas en "los términos que esta entidad los requiera".

Según concepto de la Corte, la expresión “de origen colombiano” que para el actor no concreta cual es el factor o elemento jurídico que hace una página o sitio *web* de origen colombiano, es una acusación que no está llamada a prosperar, pues en el ordenamiento legal existen disposiciones a las que no se puede acudir con el propósito de integrar su significado. Para conocer el origen de un dato electrónico se crearon criterios contenidos en la Ley 527 de 1999.

La inscripción en el registro mercantil es un acto que informa acerca de la existencia de páginas *web* o sitios de Internet que prestan servicios o realizan actividades comerciales o financieras, lo que proporciona la identificación de los agentes económicos que operan en el nuevo escenario tecnológico, de tal forma que “facilita a la administración el ejercicio de labores de control, acordes con el movimiento de la economía nacional y con las exigencias por sectores económicos”

La expresión que califica el cumplimiento del deber de informar a la DIAN de las transacciones a las que alude la norma demandada “en los términos que esta entidad lo requiera”, así formulada resulta contraria a la Constitución pues habilita a un funcionario de la administración para que señale el contenido y alcance de una obligación cuya creación y desarrollo compete a la rama legislativa del poder público y cuyos límites están determinados por la propia Constitución, particularmente por los derechos observados en la presente sentencia. Por consiguiente, las expresiones “en los términos” y “lo” contenidas en el artículo 91 de la Ley 633 de 2000, fueron declaradas inexequibles.

Sentencia C-831 de 2001. Corte Constitucional.

Magistrado Ponente. Doctor Álvaro Tafur Galvis. 8 de agosto 2001.

En ejercicio de la acción pública de inconstitucionalidad, se demandó el artículo 6º de la Ley 527 de 1999.

> *-Escrito. Cuando cualquier norma requiera que la información conste por escrito, ese requisito quedará satisfecho con un mensaje de datos, si la información que éste contiene es accesible para su posterior consulta. Lo dispuesto en este artículo se aplicará tanto si el requisito establecido en cualquier norma constituye una obligación, como si las normas prevén consecuencias en el caso que la información no conste por escrito.*

El demandante estima que la Ley 527 regula un aspecto esencial del artículo 28 de la Carta Política[116], lo cual requiere de una ley estatutaria tramitada mediante los requisitos especiales establecidos en los artículos 152 y 153 de la Constitución Política.

Al respecto la Corte consideró que los avances tecnológicos en materia de intercambio electrónico de datos requieren la adecuación de los regímenes jurídicos para ponerlos en concordancia con las transformaciones que han provocado en el ámbito social, económico y empresarial a nivel mundial.

La ley 527 de 1999 a pesar de que tiene su origen en la ley modelo, considerada de carácter internacional, y cuyos expositores pertenecen a la Comisión de

[116] Constitución Política. Art 28.-Toda persona es libre. Nadie debe ser molestado en su persona o familia, ni reducido a prisión o arresto, ni detenido, ni su domicilio registrado, sino en virtud del mandamiento escrito de autoridad competente, con las formalidades legales por motivo previamente definido en la ley. La persona detenida previamente será puesta a disposición del juez competente dentro de las 36 horas siguientes, para que este adopte la decisión correspondiente en el término que establezca la ley. En ningún caso podrá haber detención, prisión ni arresto por deudas, ni penas y medidas de seguridad imprescriptibles.

Naciones Unidas para el Derecho Mercantil, no se limitó al tema del comercio electrónico, por el contrario fue más allá, no solo regulando las operaciones comerciales sino haciendo referencia en forma genérica al acceso y uso de los mensajes de datos electrónicos.

La Corte concluye que la norma no resulta violatoria de la Constitución Nacional porque la exigencia de "escrito" no es el único requisito para privar de la libertad a una persona o allanar su domicilio, de acuerdo con una comprensión sistemática de la disposición acatada junto con el artículo 95 de la Ley Estatutaria de Administración de Justicia, donde se advierte que, la simple accesibilidad al documento para su posterior consulta no es el único requisito para reconocer la validez jurídica al mensaje de datos dentro de una actuación judicial. Asimismo no todas las materias que se refieren a un derecho fundamental deben ser objeto de la ley estatutaria. Por tanto la Corte Constitucional declaró la exequibilidad de la norma acusada.

Sentencia C-662 de 2000. Corte Constitucional.

Magistrado Ponente. Doctor Fabio Morón Díaz. Junio 8 de 2002.

En ejercicio de la acción pública de inconstitucionalidad, pide a la Corte declara inexequibles los artículos 10,11,12,13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1999.

La Ley 527 de 1999 contiene 47 artículos distribuidos en: mensajes de datos y comercio electrónico; transporte de mercancías; firmas digitales, certificados y entidades de certificación; reglamentación y vigencia.

Para efectos de este fallo se destacarán los siguientes temas: Mensajes electrónicos de datos y Comercio electrónico; las firmas digitales; las entidades

de certificación y la admisibilidad y fuerza probatoria de los mensajes de datos. El mensaje electrónico de datos se considera la piedra angular de las transacciones comerciales telemáticas.

La demandante dice cuestionar el texto íntegro de la Ley 527 de 1999, en especial los artículos antes mencionados, por estimar que violan el artículo 131 de la Carta Política así como los artículos 152 y 153.

La trasgresión del artículo 131 Constitucional, se produce, en cuanto las normas acusadas crean unas entidades de certificación, que de conformidad con la misma Ley 527 de 1999, están facultadas para emitir certificados con las firmas digitales de las personas y para ofrecer los servicios de registro y estampado cronológico, la certificación de la transmisión y recepción de mensajes de datos, autenticaciones de firmas digitales, emisión de certificados relacionados con la veracidad de firmas digitales de personas naturales y jurídicas y demás actos propios de la función fedal, lo cual es del resorte exclusivo de los Notarios, únicos depositarios de la fe pública. Por tanto, si la ley le asigna la función fedante a personas diferentes a los Notarios, infringiría en forma directa lo establecido en el artículo 131 de la Carta y esto es precisamente lo que ha hecho le ley acusada, especialmente los artículos previamente citados 2,10,11, 12, 13, 14, 15, 26, 27, 28, 29, 30, 32, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43 y 45 de la ley en comento.

Igualmente, argumenta que se incurrió en violación de los artículos 152 y 153 de la Carta Política, por cuanto sin respetar la reserva de la Ley Estatutaria ni el trámite especial, los artículos 9, 10, 11, 12, 13, 14, 15 y 28 de la Ley 527 de 1999 modificaron y adicionaron el Código de Procedimiento Civil, al conferir a los mensajes de datos la fuerza probatoria de que tratan las disposiciones del

Capítulo VIII del Título XIII, Sección Tercera del Libro Segundo del Código de Procedimiento Civil (i); ordenar que en toda actuación jurídica se de eficacia, validez y fuerza obligatoria y probatoria a todo tipo de información emitida en forma de mensajes de datos (ii); y finalmente, al disponer que los jueces deben aplicar a los mensajes de datos las reglas de la sana crítica al apreciarlos como prueba (iii).

El proyecto de ley, sigue el criterio de los "equivalentes funcionales" que se fundamenta en un análisis de los propósitos y funciones de la exigencia tradicional del documento sobre papel, para lo cual se adoptó un criterio flexible que tuviera en cuenta los requisitos de fiabilidad, inalterabilidad y rastreabilidad, aplicables a la documentación consignada sobre papel, ya que los mensajes de datos por su naturaleza no corresponden en sentido estricto a un documento consignado en papel. En conclusión, los documentos electrónicos están en capacidad de brindar los mismos niveles de seguridad que el papel, además de un mayor grado de confiabilidad y rapidez con respecto a la identificación del origen y el contenido de los datos, siempre que se cumplan los requisitos técnicos y jurídicos de ley.

Igualmente es importante valorar la admisibilidad y fuerza probatoria de los mensajes de datos: *"Los mensajes de datos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos de acuerdo al Capítulo VIII del Título XIII del Código de Procedimiento Civil".*

"En toda actuación administrativa o judicial, vinculada con el ámbito de aplicación de la presente ley, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el solo hecho de que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original". (artículo 10).

Sentencia RAD. 73-624-40-89-002-2003-053-00 del 21 de julio de 2003. Juzgado Promiscuo Municipal de Rovira (Tolima)[117]

Hechos: Al ciudadano J.S. le llegaba a su correo un sin número de mensajes donde se promocionaban servicios de la empresa Virtual Card, el manifestó no estar interesado en sus productos y solicitó su retiro de la base de datos, lo cual no fue acatado, razón por la cual instauró una tutela vía *e-mail* ante el Juez Segundo Municipal de Rovira (Tolima), requiriendo protección al derecho a la intimidad y al habeas data. El accionante considera que su correo electrónico es su domicilio virtual que está siendo atacado por actividades que atentan contra sus derechos fundamentales.

Consideraciones del despacho. El despacho determina que la tutela es viable procesalmente. Y se pronuncia: "El demandado algo extraño pues conocedor de nuevas tecnologías, precisamente porque haciendo uso de ellas se acusa de vulnerar un derecho fundamental, alega una jurisdicción material, olvidándose de la virtualidad que comprenden todas las conductas informáticas con implicaciones jurídicas".

El Juez ordenó Tutelar los derechos del habeas data, autodeterminación informática y el derecho a la intimidad del actor. Cabe resaltar que, en este país donde se violan a diario estos derechos, resulta inconcebible que la acción de tutela sea utilizada para situaciones tan superfluas, pues cuando tenemos una dirección electrónica que se encuentra en el ciberespacio, donde no existe control de la información, tenemos que someternos a que nos llegue cualquier tipo de mensajes. Sin embargo, la parte procedimental, desde la presentación de

[117] Sentencia del Juzgado Promiscuo Municipal. Juez Alexander Díaz. Acción de tutela por violación al Derecho Constitucional de Habeas Data, autodeterminación informática y la intimidad mediante spam.

la tutela vía *e-mail,* hasta la notificación del fallo igualmente por *e-mail,* es novedoso y podría ser una herramienta importante en la descongestión judicial.

STS de 12.06.07 (REC. 2249/2006; S.2.ª). Delitos contra el patrimonio. estafa//principios penales. presunción de inocencia//delitos contra el patrimonio. engaño (ri §1024518) 17/08/2007

El Supremo mantiene la condena a los acusados de un delito continuado de estafa. Son hechos declarados probados que los actores, valiéndose de un falso duplicado de la página web de un Banco habían accedido a las claves secretas de los clientes, efectuando transferencias a las cuentas abiertas por ambos recurrentes. Argumenta la Sala, respecto de la presunción de inocencia alegada por los condenados, que en el caso presente se está ante un supuesto de delincuencia económica de tipo informático de naturaleza internacional en el que los acusados ocupaban un lugar inferior y sólo tenían un conocimiento necesario para prestar su colaboración. La ignorancia del resto del operativo no borra ni disminuye su culpabilidad porque fueron conscientes de la antijuricidad de su conducta, prestando su conformidad con un evidente ánimo de enriquecimiento, ya supieran o les fuera indiferente el origen del dinero que en cantidad tan relevante recibieron.

Lo relevante es que se beneficiaron con todo, o más probablemente, en parte como pago de sus servicios, por lo que es obvio que prestaron su colaboración eficientemente en una actividad antijurídica con pleno conocimiento y cobrando por ello, por lo que no se puede alegar indefensión alguna. Sobre la alegada inexistencia de engaño por parte de los recurrentes, señala el Tribunal que dada la estructura de la estafa informática, se trata una estafa cometida a través de una transferencia no consentida por el perjudicado mediante manipulación

informática, y, en tales casos, no es preciso la concurrencia de engaño alguno por el estafador.

Sentencia 533/2007, de 12 de junio de 2007

RECURSO DE CASACIÓN Núm: 2249/2006.Ponente Excmo. Sr. JOAQUÍN JIMÉNEZ GARCÍA

En los recursos de casación por Infracción de Ley y Quebrantamiento de Forma que ante Nos penden, interpuestos por las representaciones de Roberto y Jose Daniel, contra la sentencia dictada por la Audiencia Provincial de Madrid, Sección XVI, por delito de estafa, los componentes de la Sala Segunda del Tribunal Supremo que arriba se expresan, se han constituido para la Votación y Fallo, bajo la Presidencia y Ponencia del Excmo. Sr. D. JOAQUÍN GIMÉNEZ GARCÍA, siendo también parte el Ministerio Fiscal y estando dichos recurrentes representados por los Procuradores Sr. Cobo Martínez de Murguia y Sr. Esteban Sánchez; siendo parte recurrida Citibank España S.A., representado por el Procurador Sr. Barreiro-Meiro Barbero.

I. ANTECEDENTES

"1º.- Luis, menor de edad y contra el que no se sigue este procedimiento propuso al acusado Augusto, con ordinal de informática NUM000, mayor de edad y sin antecedentes penales, un negocio consistente en abrir una cuenta corriente en el Citibank donde recibiría diversas transferencias con cargo a otras cuentas a las cuales el menor, puesto de acuerdo con unos individuos desconocidos, accedía a ellas enviando diversos correos electrónicos a clientes de Citibank con un falso duplicado de su página web haciéndose pasar por empleados para conseguir las

claves secretas y una vez sabidas, ordenaba las falsas transferencias a favor de las cuentas, tanto de Augusto como de los acusados Pedro Francisco y Evaristo, ambos mayores de edad y sin antecedentes penales, que fueron convencidos por Augusto para la apertura de cuenta y recepción de las transferencias. De esta forma aperturaron las cuentas e ingresaron en ellas un total de 159.559,20 y 73.197,77 euros respectivamente. En el momento de la detención se le intervinieron diversas tarjetas de visita, entre otros del Citibank, varias tarjetas visa y 650 euros.-és de transferencias, la cantidad de 14.866,75 euros de los que no dispuso de 4,04. Cuando se le detuvo se le intervino diversa documentación bancaria.- d) Pedro Francisco: el día 19.1.2004 en la sucursal núm. 10 de la calle Princesa de Madrid, aperturó una cuenta e ingresó en ella, por el mismo procedimiento, la cantidad total de 18.016,37 euros de los que no dispuso de 2027,97 euros. Cuando se le detuvo le intervinieron diversos documentos bancarios, igualmente, recibió varias transferencias por importe total de 27.769,21 euros de los que dispuso.- dichas cantidades las obtuvieron de cuentas corrientes de clientes de Citibank en E.E.U.U. a través de la banca on-line, cantidades que fueron compensadas bancariamente por el Centro Compensador de Citigroup en Long Island City de Nueva York.- El Banco ha abonado a todos sus clientes el importe de las anteriores transferencias.

Segundo.- La Audiencia de instancia dictó el siguiente pronunciamiento:

“FALLAMOS: Que debemos CONDENAR Y CONDENAMOS como responsables en concepto de autores de un delito continuado de estafa, ya definido, a la pena de prisión de tres años, multa de ocho meses con cuotas de tres euros; a inhabilitación especial para el derecho de sufragio pasivo durante el tiempo de la condena y pago de una novena parte de las costas causadas.

Se está ante un caso de delincuencia económica de tipo informático de naturaleza internacional en el que los recurrentes ocupan un nivel inferior y sólo tienen un conocimiento necesario para prestar su colaboración, la ignorancia del resto del operativo no borra ni disminuye su culpabilidad porque fueron conscientes de la antijuridicidad de su conducta, prestando su conformidad con un evidente ánimo de enriquecimiento, ya supieran, no quisieran saber --ignorancia deliberada--, o les fuera indiferente el origen del dinero que en cantidad tan relevante recibieron. Lo relevante es que se beneficiaron con todo, o, más probablemente, en parte como "pago" de sus servicios, es obvio que prestaron su colaboración eficiente y causalmente relevante en una actividad antijurídica con pleno conocimiento y cobrando por ello no pueden ignorar indefensión alguna, por su parte la "explicación" que dieron de que no pensaban que efectuaban algo ilícito es de un angelismo que se desmorona por sí sólo. En la sociedad actual el acervo de conocimientos de cualquier persona de nivel cultural medio conoce y sabe de la ilicitud de una colaboración que se le pueda pedir del tipo de la que se observa en esta causa, y al respecto, hay que recordar que los recurrentes vivían en Madrid y no consta en los autos nada que pudiera ser sugestivo de un desconocimiento de la ilicitud de la colaboración que se le pedía, máxime cuando no se trataba de una colaboración gratuita sino que llevaba aneja un claro enriquecimiento personal. No hay por tanto ninguna posibilidad de derivar a ningún supuesto de error la acción de los recurrentes.

Sobre la inexistencia de engaño por parte de los recurrentes, sólo recordar que dada la estructura de la estafa informática, y estamos en una estafa cometida a través de una transferencia no consentida por el perjudicado mediante manipulación informática, en tales casos no es preciso la concurrencia de engaño alguno por el estafador. En tal sentido, STS de 20 de Noviembre de

2001 y ello es así porque la asechanza a patrimonios ajenos realizados mediante manipulaciones informáticas actúa con automatismo en perjuicio de tercero, precisamente porque existe la manipulación informática y por ello no se exige el engaño personal. No hubo vacío probatorio sino prueba de cargo válida y suficiente que fue razonada y razonablemente motivada.

En conclusión no existe ninguno de los vicios procesales denunciados.

III. FALLO

Que debemos declarar y declaramos NO HABER LUGAR a los recursos de casación formalizados por las representaciones de Roberto y Jose Daniel, contra la sentencia dictada por la Audiencia Provincial de Madrid, Sección XVI, de fecha 6 de Julio de 2006, con imposición a los recurrentes de las costas de sus recursos.

12. CONCLUSIONES

- Existe un extenso número de comportamientos que no han sido tenidos en cuenta por la doctrina debido a la confusión de conceptos, cuyo objeto "material" es informático, razón por la cual es importante que se haga una precisión técnica legislativa a fin de facilitar un juicio de adecuación típica.

- En Colombia no tenemos un desarrollo amplio de la doctrina sobre la materia, y mayormente debemos referirnos al derecho comparado, escrito en países de mayor tradición jurídica sobre el tema, con el fin de combatir los altos índices de criminalidad y no ver vulnerados los derechos de las personas naturales y jurídicas nacionales e internacionales.

- Si bien es cierto que las entidades gubernamentales deben abrir paso a las nuevas tecnologías, hacia la modernización de sus dependencias, es evidente el alto grado de criminalidad existente en nuestro país, lo que conlleva a que las instituciones responsables reglamenten y limiten el acceso indiscriminado a cualquier dato o información personal que pueda ser utilizado para actos delictivos causando daño a una persona.

RECOMENDACIONES

- Es necesario realizar una valoración de la legislación colombiana frente a tales comportamientos y conductas atípicas de los delitos informáticos para proyectar una nueva reforma al Código Penal, tipificando esa nueva

modalidad de delitos que se están presentando con la utilización de los sistemas en red y la Internet.

- Se debe hacer un análisis comparativo de la legislación nacional con las legislaciones de países desarrollados de Europa, especialmente la de Alemania, la de Estados Unidos y España, puesto que le han dado mayor énfasis al estudio de estos temas debido a la alta cifra de criminalidad combinadas con las pérdidas económicas en que han incurrido múltiples empresas ante todo entidades financieras.

- Pretendemos crear el interés de Universidades, investigadores, estudiantes, magistrados, jueces, abogados que proyecten y amplíen el tema en cuestión, para que en el futuro tengamos una legislación unificada acorde con los principios de globalización.

13. BIBLIOGRAFÍA

BALMA CEDA HOYOS, Gustavo. Delito de estafa informática. Editorial Leyer. 2008.

BOTERO, Luís Felipe y otros. Comercio electrónico en Colombia. Principales aspectos legales. Primera edición. Bogotá, Baker & McKenzie, 2002.

CHOCK Patricia. El uso de los computadores en la explotación sexual de los niños y en la pornografía infantil.

CODIGO DE PROCEDIMIENTO CIVIL. Bogotá. Ediciones Legis 2000.

CODIGO PENAL. Bogotá, Editorial temis. 2002.

CODIGO DE COMERCIO. Decreto 410 de 1971.

CONSTITUCION POLITICA DE COLOMBIA. Bogotá, Editorial Temis. 2002.
Convención Americana sobre Derechos Humanos. Pacto de San José. Artículo 13. Ley 16 de 1972.

Declaración Universal de los Derechos del Hombre. Constitución Política de Colombia. Bogotá. Legis 2000.

DEL PESO NAVARRO, Emilio. Socio Director de Informáticos Europeos Expertos. Contratos Informáticos. Internet, Lima.

DESANTES, José María, Fundamentos del derecho de la información, Ed. Confederación Española, Madrid 1977.

ENCICLOPEDIA ENCARTA 2006.
Gaceta Constitucional Nº 82, pág 12. Constitución Política de Colombia. Origen, evolución y vigencia. Bogotá, Diké, 1996.

Gaceta Constitucional Nº 127.

GONZALEZ, Cristóbal, De la libertad de expresión a la libertad de información, Revista Universidad INCCA, abril de 1992. Bogotá.

GUERRERO MATEUS, María Fernanda y SANTOS MERA, Jaime Eduardo. Fraude Informático en la Banca. Pág 75.

GUTIERREZ GOMEZ, María Clara. Internet Comercio Electrónico & Telecomunicaciones e Informática, Cap: Consideraciones sobre el tratamiento jurídico del comercio electrónico. Bogotá: Legis 2002.

HEGEL, W. Lecciones sobre la historia de la filosofía, Tomo I. México 1977.

KOSIUR David**,** Understanding Electronic Commerce. Redmon. Press. 1997.

LEE TIEN. La sexualidad infantil y las nuevas tecnologías de la información. Universidad de California. Traducción del profesor JOSE LUIS ARAMBURO RESTREPO Facultad de Derecho. Universidad Nacional. Bogotá. 1995

LEON MONCALEANO, William Fernando. De la Comunicación a la Informática Jurídica Penal Bancaria.Ed. Doctrina y Ley Ltda.. Bogotá 2001.
Ley 527 de 1999.

Ley de rectificación, artículo 20.

MADRID-MALO, Mario. Estudios sobre derechos fundamentales. Bogotá, Tercer Mundo, 1995.

MARQUEZ ESCOBAR, Carlos Pablo. El delito informático. Bogotá. Ed. Leyer.

MENDOZA PALOMINO, Álvaro. Teoría y Sinopsis de la Constitución de 1991. Bogotá, Doctrina y Ley, 1992, pág 245.

ORGANIZACIÓN MUNDIAL DEL COMERCIO, Estudios Especiales 2. El Comercio Electrónico y el papel de la OMC. Instrumentos del Comercio Electrónico.

RENGIFO GARCÍA Ernesto, Nuevos Retos del Derecho Comercial, Comercio Electrónico, Documento Electrónico y Seguridad Jurídica, Primera edición, Biblioteca Jurídica Dike, 2000.

RINCON CARDENAS, Erick. Manual de derecho de comercio electrónico y de Internet. Bogotá, Centro Editorial Rosarista, Facultad de Jurisprudencia, 2006.

RIVERA LLANO Abelardo. Dimensiones de la informática en el derecho. Perspectivas y problemas. Editorial Jurídica Radar. Bogotá 1985.

Resolución 51/162 de 1996.

SARZANA, Carlos. Note Sul Diritto Penale dell´ informática. Giust Penale.1984

Sentencia 662 de 2000 Magistrado Ponente Dr Fabio Moron Diaz,. Corte Constitucional. Comisión de Naciones Unidas para el desarrollo del Derecho Mercantil Internacional- UNCINTRAL.

Sentencia T-729 de 2002 de la Corte Constitucional**.**

Sentencia RAD. 73-624-40-89-002-2003-053-00 del 21 de julio de 2003. Juzgado Promiscuo Municipal de Rovira (Tolima).

Sentencia del Juzgado Promiscuo Municipal. Juez Alexander Díaz. Acción de tutela por violación al Derecho Constitucional de Habeas Data, autodeterminación informática y la intimidad mediante spam.

TELLEZ VALDEZ, Julio. Derecho informático.

TORRES TORRES, Henry William. Derecho informático.Bogotá. Ediciones Jurídicas, 2002.

VALENCIA ZEA, Arturo, ORTIZ M, Alvaro. Derecho Civil. Parte General y Personas. Temis 1994.

Vattier Fuenzalida Carlos, Instituciones del Derecho Privado – Contratación Contemporánea, Palestra editores Lima– Editorial Temis S.A. Bogotá, 2001.

Wierner, N. *Cybernethic,. Cambridge. Mass: M.I.T. Press,* 1948, citado por CROSSON, F.y SAIRE, K, *Filosofía y Cibernetica,* México, Fondo de la Cultura Económica, 1982

14. WEBGRAFIA

http://www.salvador.edu.ar/castoldi.htm. Aspectos legales derivados de la Implementación de Sistemas Informáticos. 26 de mayo de 2003.

http://es.wikipedia.org/wiki/November 2006 Defraudaciones and Telecomunicaciones/

http://es.wikipedia.org/wiki/unique-root-draft.hml.

htpp://www.dlmforum.eu.org.

http://es.wikipedia.org/wiki/pishing=cite-note-1.

http://es.wikipedia.org/wiki/pishing=cite-note4

http:// www. eltiempo.com/Colombia/justicia/